Araştırma Makalesi/Research Article

E-Devletin Güvenlik Bağlantılı Sorumlulukları ve E-Vatandaşın Hakları

Security-related Responsibilities of the E-Government and The Rights of the E-Citizen

Zerrin Toprak KARAMAN *

Öz

E-Devlet, kamu yönetimi teşkilatlanmasının yürüttüğü kamu hizmetleriyle doğrudan ilgili bir kavramdır. Planlamadan kontrole, yönetim süreci aşamalarının desteklenerek kamu hizmetlerinin kalitesini ve verimliliğini artırmak için başvurulan dijital bir yöntemdir. Dijital kamu hizmetleri, halk ve idareler arasındaki etkileşimi daha hızlı, daha az pahalı, verimli, izlenebilir ve rahat yapılabilir hale getirerek, kurumlar ve bireylerin karşılıklı yükünü azaltmaktadır. Ayrıca, dijital teknolojilerin kullanılması yoluyla, devletin modernleşmesi stratejilerini bütünleştirerek, topluma ekonomik ve sosyal fayda yaratması hedeflenmektedir. Felsefesi gereği, kurumlar arası işbirliğini de sağlamaktadır.

E-Hizmetler yoluyla, "devlet" ve "vatandaş" ilişkilerinin planlaması ve yöne-timi giderek kamu yönetimlerinin yapılanma çalışmalarının merkezinde yer almaya başlamıştır. Bu yöndeki uluslararası çalışmalar incelendiğinde birçok ülkenin, yöne-timde doğrulanmış bilgi akışına dayalı verimliliği sağlamak amacıyla çeşitli adlar al-tında, devletten vatandaşa internet erişimleri sağlama uygulamalarını hızlandırdığı anlaşılmaktadır. Halka yönelik açıklamalarda, e-kamu hizmetleri yapılanmasında he-deflenen amacın, ihtiyaç duyulan bilgiye hızla ve kolaylıkla erişebilme imkânı; Vergi ödemeleri, lisanslar, pasaport alma gibi işlemleri desteklemede kolaylıklar sağlandığı belirtilmektedir. Faydayı çoğaltan yönde etkileri için de; yönetime katılım ve idareyle etkileşimin kolaylaşması yanında, halkın yönetime katılımı ve hizmetlerin kalitesinin artması beklenmektedir. İdarenin halka bilgi vermesinin sağladığı etkileşim ile vatandaşların hukuki düzenlemeler, hizmetler ve politikaları hakkında daha bilinçli olmalarının sağlanacağına vurgu yapılmaktadır. Vatandaş için, e-devlet yönetimi ve hizmet-leri: kamu politikasına ilişkin bilgiler, istihdam ve iş fırsatları, oylama bilgileri, vergi beyannamesi, lisans tescil veya yenileme, para cezalarının ödenmesi ve sunulması gibi çok çeşitli bilgi ve hizmetlere erişim fırsatı yanında; bu yöndeki çalışmaların çevre koruyucu politikalara da hizmet edeceği, kamu yönetiminin ülke bütününde oluşan rakamsal analizlere dayanarak daha etkin çalışmasına yardımcı olabilecek yeni taktik-ler ve stratejiler oluşturabileceği anlamına da gelmektedir.

Bu makalenin hedeflediği amaç, e-devletin sorumlulukları ile e-vatandaş haklarının, modern güvenlik tanısı kapsamında, 2018 tarihinde uygulamaya giren Türki-ye Başkanlık modeliyle ilişkilendirilerek incelenmesidir.

Geliş Tarihi/Received: 10.02.20120 - Kabul Tarihi/Accepted: 05.03.2020

* Prof. Dr. Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi Bölümü, zerrintoprak@gmail.com, ORCID: 0000-0001-8724-1306.

Anahtar Kelimeler: E-Devlet, Siber Güvenlik Ekosistem, E-Vatandaşın Hakları, E-Demokrasi, e-Yönetişim.

Abstract

E-government is a directly related concept to public services carried out by public administration. It is a digital method that is used to increase the quality and efficiency of public services by supporting the phases of administration process from planning to control. Digital public services, reduce the mutual burden of institutions and individuals by making the interaction between public and government faster, less costly, efficient, traceable and comfortable. In addition, through the use of digital technologies, it is ai-med to integrate the modernization strategies of the state and create collective economic and social benefits. It's philosophy also provides cooperation between institutions.

Through E- Services, the planning and administration of "government" and "citizen" relations has gradually begun to take place at the center of public administration's struc-turing efforts. When international studies in this area are examined, it is understood that many countries accelerate the implementation of providing internet access to citizen under various names in order to provide efficiency on verified information flow in administration. In public explanations, the aim of e-public services structuring is the ability to quickly and easily access the information needed; It is stated that facilities are provided to support the operations such as tax payments, licenses, passports. Consequ-ently, it is expected that the participation of the people and the quality of the public services will increase. It is emphasized that the interaction provided by informing the public will enable citizens to be more conscious about legal regulations, services and policies. For citizens, e-government administration and services are; access to a wide range of information and services such as public policy information, employment and business opportunities, voting information, tax declaration, license registration or re-newal, payment of fines and submission. Again, it also means that the work in this area will serve environmental protection policies and will create new tactics and strategies that can help public administration to work more effectively based on numerical analy-zes that are made throughout the country.

This article aims to target the state examination in association with modern security responsibilities and recognize the rights of e-citizens which associated with the presi-dential administration Turkish model entered into force in 2018.

Keywords: E-Government, Cyber Security Ecosystem, E-Citizen's Rights, E-Democracy, E-Governance.

GİRİŞ

Dünyamız, günümüzde geçmişte olduğundan daha da fazla, her türlü bilgiye hızla ulaşma yanında mal ve hizmetin dolaşımı anlamında, küçülmüştür. Dijital teknoloji sayesinde binlerce kilometre boyunca gerçek zamanlı bağlantı kurulabilir hale gelmiştir. Teknolojik gelişmeler sayesinde hızla ve dünyanın bir ucundan diğerine alışveriş yapabilme, çalışmaları etkin yürütebilme, bilgiye erişme, ulusal ve uluslararası etkileşimde bulunabilme imkânı sağlanmıştır. İnsanlar, bireysel veya örgütsel, birbiriyle her zamankinden daha fazla irtibatlaşırken, küreselleşmenin temel unsurları olan iletişim ve ekonomi de birbirleriyle bağlantılı büyümeye devam etmektedir. Kamu yönetimi ilkesel olarak, yenilikleri vatandaş ve kamu hizmetlerinden yararlananlar açısından, titizlikle yakından takip ederek özel sektör yaklaşımına uygun hizmet verimliliğini artırmaya çalışmaktadır. Ancak artan oranda yenilik, artan oranda risk ile birlikte gelmektedir.

Tarih boyunca insanlığı olumsuz etkileyen ve büyük rakamlarla ölümle sonuçlanan çeşitli salgınlar, soygunlar vb. vakalar günümüzde bilgisayar ortamında da virüs, çevrim içi soygunlar gibi benzer etkiler yaratabilecek bir özellik taşımaktadır.

Nitekim iyi eğitimli teröristler ve insan tacirleri gibi insani tehdit unsurları, sürekli gelişen yeni teknolojik imkânları kullanarak, yurt dışından fiziksel sınırların ihlalini yapabildiği gibi, yurt içinden de tehdit ve tehlike oluşturabilmektedir. Bu nedenle güvenliği sağlamak için uluslararası ortaklık ile bütünleşik sınır yönetimi modeli geliştirilmiştir. Dış sınırlarda yüksek güvenlik unsurlarını oluşturmak ve göç hareketlerini düzenlemek amacıyla geliştirilmiş ve yetkili kuruluşları işbirliği ve koordinasyona davet etmiştir. Bu yaklaşımın benimsettiği temel felsefe gereği dünya ülkeleri en azından bölgesel ortaklıklardan başlayarak, "bütünleşik e-güvenlik / e-siber sınır yönetimi" sürecine doğru adım adım gitmektedir.

Terör, yarattığı travma ve yıkıcı etkiler nedeniyle günümüzde her gün bir başka ülkede karşılaşılan insan kaynaklı afet tipidir. Dünya Sağlık Örgütü (WHO) tanımına göre de, "herhangi bir olay zarara, ekonomik bozulmaya ve kayıplara, insan hayatı, sağlığı ve sağlık hizmetlerinin bozulmasına neden olursa, afet olarak nitelendirilmektedir. Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) dokümanlarında, 2013 tarihli Türkiye Afet Müdahale Planı (Afet ve Acil Durum Yönetim Başkanlığı, 2013, s. 6) afet tipleri ve hizmetlerin belirtilmesine yönelik hazırlanan tablo içeriğinde, doğrudan "terör" sözcüğü geçmemekle birlikte, siber saldırılara yer verilmiştir. İnsan kaynaklı siber saldırılar, bilgi ve teknolojinin terörist amaçla kullanımı olarak literatürde tanımlanmaktadır.

Terörist saldırılar günümüzdeki örnekleri de dikkate alınarak; bizzat hedefe doğrudan saldırı ile doğal afetler sırasında oluşan kaotik ortamdan yararlanılarak gerçekleştirilen terörist saldırılar olarak kendi içinde gruplandırılabilir. Terörist saldırılar nedeniyle ortaya çıkan endüstriyel, nükleer vb. kazalar insan eliyle yaratılan afetler olarak değerlendirilmektedir. Ayrıca, terörist saldırılar, yarattığı sektörel tehditler yanında, doğrudan insan varlığına zarar vererek sebep olduğu maddi ve manevi kayıplar nedeniyle devlete/topluma karşı işlenmiş suçlar olarak insan kaynaklı afetlerdir. Günümüzde yaşanan terör olayları nedeniyle halka tavsiye edilen, evde 3 günlük gıda, su bulundurulması, elektrik kesintilerine karşı pilli radyo vb, tedbirler, tıpkı afet tedbirleri gibi listelenmektedir. Aşağıda temel insan kaynaklı afetlere yer verilmiştir.

1. Nükleer, biyolojik, kimyasal kazalar,
2. Taşımacılık kazaları,
3. Endüstriyel kazalar,
4. Ulaşım kazaları,
5. Aşırı kalabalıktan meydana gelen kazalar,
6. Büyük rakamlara ulaşan göçler.
7. Siber saldırılar

3713 sayılı Terörle Mücadele Kanununa göre terör tanımı; "Cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek,

Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir(3713 sk, md.1). Bu maddede belirlenen amaçlara ulaşmak için meydana getirilmiş örgütlerin mensubu olup da, bu amaçlar doğrultusunda diğerleri ile beraber veya tek başına suç işleyen veya amaçlanan suçu işlemese dahi örgütlerin mensubu olan kişi terör suçlusudur. Terör örgütüne mensup olmasa dahi örgüt adına suç işleyenler de terör suçlusu sayılır (3713 sk, md. 2). Terörist saldırılar, yurt içinden veya yurt dışından, sınır ötesinden gelebilir ve afet yönetimi risk analizleri içinde terör unsuru giderek daha fazla yer almaktadır.

2003 tarihli ve 4800 sayılı Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesi gereğince, Bir suçun "sınıraşan" niteliği kazanması için "birden fazla ülkede işlenmesi veya bir ülkede işlenmekle birlikte hazırlık, planlama, yönetim veya kontrolü gibi (yönetim süreçlerinden birkaçı veya tümünün) bir başka ülkede yapılmış olması veya bir devlette işlenmekle birlikte suçun içinde yer alan organize suç grubunun birden fazla devlette faaliyette bulunması veya bir devlette işlense bile etkisinin başka devletlerde de görülebiliyor olması" (Türkiye Büyük Millet Meclisi md.3 , 2003) gerekmektedir. Bu tanım unsurları itibariyle incelendiğinde, mutlaka zarar gören ülke dışından bir zarar getirici müdahale gerçekleşmektedir. Zarar getiren de (ülke) yasal olmayan bir müdahaleden, kabul edilmiş dünya çapında etik değerler yönüyle, izlenebilir bir ortamda itibar açısından zarar göreceği açıktır. Ülkeye zarar getiren olgusallıklar, terör ile ilişkilendirilmektedir.

Kamu yönetimi de, hizmet alanlara yönelik hizmetlerde faydayı artırma ve demokratik katılım unsurlarını işlevsel kılma amaçlı dijital çalışmaları önemsemektedir. E-devlet, kamu yönetimi teşkilatlanmasının yürüttüğü kamu hizmetleriyle doğrudan ilgili bir kavramdır. Yönetim süreçlerinin, planlamadan kontrole desteklenerek kamu hizmetlerinin kalitesini ve yürütülmesinde verimliliği artırmak için dijital yöntemler kullanılmaktadır. Dijital kamu hizmetleri, halk ve idareler arasındaki etkileşimi daha hızlı ve verimli, daha az pahalı, erişilebilir, izlenebilir ve kolay yapılabilir hale getirerek, kurumlar ve bireylerin karşılıklı yükünü azaltmaktadır. Ayrıca, dijital teknolojilerin kullanılması yoluyla, devlet teşkilatının işletim mekanizmalarının modernleşmesinin, topluma ekonomik ve sosyal fayda yaratması hedeflenmektedir. Felsefesi gereği, e-irtibat kurumlar arası işbirliğini de sağlamaktadır.

E-HİZMETLER

E-Hizmetler yoluyla, "devlet" ve "vatandaş" ilişkilerinin planlaması ve yönetimi giderek kamu yönetimlerinin yapılanma çalışmalarının merkezinde yer almaya başlamıştır. Bu yöndeki uluslararası çalışmalar incelendiğinde birçok ülkenin, yönetimde doğrulanmış bilgi akışına dayalı verimliliği sağlamak amacıyla çeşitli adlar altında, devletten vatandaşa internet erişimleri sağlama uygulamalarını hızlandırdığı anlaşılmaktadır. Halka yönelik çalışmalar; e-kamu hizmetleri yapılanmasında hedeflenen amacın, ihtiyaç duyulan bilgiye hızla ve kolaylıkla erişebilme imkânı yönüyle; vergi ödemeleri, lisanslar, pasaport alma gibi işlemleri desteklemede kolaylıklar sağlanmaktadır. Faydayı çoğaltan yönde etkileri için de; yönetime katılım ve idareyle etkileşimin kolaylaşması yanında, halkın yönetime katılımı ve hizmetlerin kalitesinin artması beklenmektedir. İdarenin halka bilgi vermesinin sağladığı etkileşim

ile vatandaşların hukuki düzenlemeler, hizmetler ve politikaları hakkında daha bilinçli olabileceği beklenmektedir.

Vatandaş için, e-devlet yönetimi ve hizmetleri: kamu politikasına ilişkin bilgiler, istihdam ve iş fırsatları, oylama bilgileri, vergi beyannamesi, lisans tescil veya yenileme, para cezalarının ödenmesi gibi çok çeşitli bilgi ve hizmetlere erişim fırsatıdır. Ayrıca, e- çalışmaların doğal çevreyi koruyucu politikalara da hizmet edeceği, kamu yönetiminin ülke bütününde oluşan rakamsal analizlere dayanarak daha etkin çalışmasına yardımcı olabilecek yeni taktikler ve stratejiler oluşturabileceği anlamına da gelmektedir.

Hizmet tanımlamaları vatandaş odaklı olmakla birlikte, küreselleşme dinamikleri ve insan hakları tanısı bağlamında, bir ülkenin vatandaşı bir başka ülke de güvenli yaşayabilme haklarına ya da güvencesine sahiptir. Yerleşik yabancı statüsündeki bireyler, ülkeden ülkeye değişen kısıtlar olsa da, örneğin mülkiyet ilişkileri nedeniyle vatandaş ile özellikle borçlar açısından çoğu kere benzer sorumluluklara sahiptir ve e-hizmetlerinin tamamen dışında değildirler.

Türkiye'de 2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu, 2000'li yılların başında yürürlüğe giren temel bir demokratik düzenlemedir. Dönemi itibariyle, Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkındaki 2011 tarihli Kanun Hükmündeki Kararname (KHK/655) hükümlerine göre; "Bilgi toplumu politika, hedef ve stratejileri çerçevesinde; ilgili kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonu sağlayarak e-Devlet[1] hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirlemek, bu hizmetlere ilişkin eylem planları yapmak, koordinasyon ve izleme faaliyetlerini yürütmek, gerekli düzenlemeleri yapmak ve bu kapsamda ilgili faaliyetleri koordine etmek (655 KHK, md.2/f)" çalışmaları ile e-Devlet felsefesi oluşturulmuştur.

2018 yılı itibariyle yürütülen yeniden yapılanma çalışmaları bağlamında, Ulaştırma ve Altyapı Bakanlığının teşkilatlanmasında, Haberleşme Genel Müdürlüğü, e-devlet ve siber güvenlik konularında yetkilidir. 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve e-Devlet bağlantılı gerekli düzenlemeler, uluslararası alandaki gelişmelere uygun çalışmalarla yürütülmektedir. Veri güvenliğini sağlama ile yetki ve sorumluluk, 6698 sayılı kanunla, Cumhurbaşkanının görevlendireceği bir bakan sorumluluğunda, idari ve mali özerkliğe sahip kamu tüzel kişiliği olan "Kişisel Verileri Koruma Kurumu" ile ilişkilendirilen (md.19) bir yapılanmadan oluşmaktadır. Ayrıca bu yapılanmada "Kişisel Verileri Koruma Kurulu Başkanı" ve "Veri Sorumlusu", açısından doğrudan veri güvenliğinin sağlanmasına ilişkin yetki, görev ve sorumluluklar bulunmaktadır.

E-kamu çalışmaları genel olarak bilgi alan, mevzuatla belirtilen idari ve mali hizmetlerin hızlı yürütülme özelliğinin sağlanmasına ilişkin ilkeleri ağır basan bir yönetim sürecidir. Nitekim, 2005 tarihli ve 5393 sayılı Belediye Kanunu'na 2018 yılında eklenen Ek Madde 3 (Ek: 15/2/2018-7099/16 md.) düzenlemesine göre; "Belediyeler, mevzuatla kendilerine verilen görev ve hizmetlerin yürütülmesi ve vatandaşlar tarafından yapılan başvuruların sonuçlandırılması amacıyla her türlü idari iş ve işlemin yürütüldüğü e-Belediye bilgi sistemini kullanır. E-Belediye bilgi

[1]E-devlet şifresi 15 yaşını doldurmuş Türkiye Cumhuriyeti vatandaşları ve Türkiye'de ikamet eden veya çalışan yabancılar tarafından alınabilir.

sistemini kurmaya, işletmeye, veri saklama, veri iletimi ve veri paylaşımı ile ilgili politikaları tespit etmeye, çalışma usul ve esaslarını belirlemeye ve bu sistem ile ilgili merkezî bir hizmet standardizasyonu oluşturmaya İçişleri ile Çevre ve Şehircilik bakanlıkları müştereken yetkilidir".

3 Eylül 2016 tarihli 29.820 sayılı Resmi Gazetede yayınlanan, "E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik" hükümlerine göre; "e-Devlet hizmeti: Hizmet süreçlerinin vatandaş odaklı olarak yeniden yapılandırılmasını da içerecek şekilde, kurumlar arası veri paylaşımı esasına dayalı olarak yürütülmesi için kurumlar tarafından, hızlı, güvenli, etkili, verimli, şeffaf ve hesap verebilir, temel hak ve özgürlüklere riayet edilerek ve mahremiyet gözetilecek şekilde elektronik ortama aktarılan her bir kamu hizmetini" (Yönetmelik, md.4/c) tanımlamaktadır. Ayrıca gerekli çalışmalara devam edileceği, e-devlet hizmetlerinin sunulmasında ilkeler ile bakanlığın, kamu kurum ve kuruluşlarının ve e-devlet kapısı işletmecisinin görev ve sorumlulukları listelenmiştir. E-devlet sorumlulukları 14 madde ile belirlenmiştir.[2] E-devlet kapısının güvenliği, bilgi güvenliğine yönelik ihlaller ve kök nedenler, kullanıcının"şifresini kimseyle paylaşmamak koşulu ile geçerli "şifre güvenliği" sorumluluğu gibi ilkeler, bilginin güvenliğini sağlamaya yönelik yada güvenli bağlantı üzerine oluşturulmuştur. Vatandaşın hakları konusu için bir başlık açılmamıştır.

E-devlet çalışmaları, internet ortamında kamu hizmetlerini etkin yönetebilmenin teknolojik boyutudur. Belirtilen bu çok yönlü gelişmeyi yönetebilmek ya da böyle bir yöntem tercihinin nedeni olan başarıyı sağlamak için temel ilkelerin oluşturulması ve uzun vadeli bir vizyona dayalı e-Devlet eylem planı oluşturulması gerekmektedir. E-Devletin, yurttaşlara, işletmelere ya da iş dünyasına, yabancılara ve toplamda kısaca halka getirebileceği önemli faydaları sağlamak amacıyla ne tip girişimler planlanacak ve yönetilecektir soruları çalışmaların temelini oluşturmaktadır. E-devlet çalışmaları sayesinde, Devletin yönetim tarihi gelişme sürecindeki demokratikleşme çabalarının sonucu olarak, vatandaşı kendisinden sadece bilgi alınan ancak bilgi verilmeyen bir konumdan çıkmakta ve bilgiyi vatandaşla paylaşan bir yönetim yapılanması geliştirilmektedir.

VİZYON VE TEMEL İLKELER

Kamu hizmetlerini sürekli olarak iyileştirmek için e-devleti kullanan "idarenin", öncelikle vatandaşlar olmak üzere halk, kurum ve kuruluşlar ile olan ilişkilerinde, şeffaf olması ve işbirliği yapması istenmektedir. Bu çalışmalarda izlenecek yöntemin belirlenmesine ilişkin Avrupa Birliği tarafından geliştirilmiş ve 2020 yılına kadar kamu idareleri ve kamu kurumları için hedef konuları; dokümanların izlenebilir, anlaşılabilir, açık, verimli ve kapsayıcı olması(European Union, 2016) hususudur. Avrupa Konseyinde de geliştirilen çalışmalar, yönetişim ve demokratik devlet konularında tasarlanmış kurumsal iyi çerçeve örnekleri sunmaktadır. Avrupa Konseyi 2000'li yılların başında temel düzenlemeleri demokrasi unsurları açısından

[2] E-devlet sorumlulukları, 15.04.2019 tarihinde https://www.turkiye.gov.tr/bilgilendirme?konu=politikalar adresinden alındı.

geliştirmiştir. Nitekim Bakanlar Komitesi Tavsiye Kararı Rec (2004) 15 ile elektronik yönetişim (e-governance), Tavsiye Kararı Rec (2004)11 ile yasal, operasyonel ve teknik standartlar için, e-oylama (on legal, operationalandtechnicalstandardsfor e-voting) ve e-demokrasi (e-democracy) Rec (2009)1 yapılabilirliği için uzun ancak etkili bir yol alınmıştır. Bu düzenlemeler uluslararası E-devlet çalışmalarına başlangıç olarak önem taşımaktadır.

E-demokrasi ile ilgili tavsiye kararında yer alan ilkeler incelendiğinde, E-devlet çalışmalarında temel referans olduğu anlaşılmaktadır (Council of Europe, 2009) Belirtilen düzenlemeye göre;

"E-demokrasi; demokrasi, demokratik kuruluşlar ve demokratik süreçlerin güçlenmesinde bilgi ve iletişim teknolojisinin fırsatları kullanılmasında kullanılan stratejik bir yaklaşımdır. E-demokrasi, toplumların demokratik, insani, kültürel ve etik değerleri üzerine dayanmaktadır ve aynı zamanda iyi yönetişim ile de yakın bir ilişki içindedir.

E-demokrasi, bilgiye erişmede, temel özgürlükler, insan hakları ve azınlık haklarına da saygı gösterme fikrine dayanmaktadır. E-demokrasi, demokrasinin tüm sektörleri, tüm demokratik kuruluşlar, her düzeyde yönetimler ve geniş çapta tüm kurumlarla ilişkilidir. E-demokrasinin paydaşları demokrasiden yarar sağlayan tüm bireyler ve kuruluşları kapsamakta, çeşitli paydaşlar arasında işbirliğini gerektirmektedir. Sadece yönetimler değil, vatandaşlar ve sivil toplum kuruluşları da bu işbirliğine dâhildir. Bu yüzden e-demokrasi hakkında yapılan öneriler tüm paydaşları kapsamaktadır.

E-demokrasi ile bilginin elde edilmesi, iletişim, danışma, müzakere, birlikte karar verme gibi konularda paydaşlar arasında işbirliğinin gerçekleşmesini sağlanacaktır. E-demokrasi disiplinlerarası ve sınır aşan bir araştırma gerektirecektir. E-demokrasi aynı zamanda yeni teknolojiler ile gençlerin de demokrasiye, demokratik kuruluşlara ve süreçlere ilgisini çekecektir. E-demokrasi bilgi teknolojileri sayesinde politika oluşturmada politikacıları ve vatandaşları bir araya getirecektir. Politikaların beraberce oluşturulması demokrasiye olan güveni artıracaktır. E-demokrasi birey ve grupların seslerini daha iyi duyuracaktır.

E-demokrasi, e-parlamento, e-yasama, e-yargı, e-uzlaştırma, e-çevre, e-seçim, e-referandum, e-oylama, e-müzakere, e-kampanya, e-dilekçe, e-seçimi içine alarak elektronik katılımı, müzakereyi ve forumları mümkün kılmaktadır. Bunlar arasında e-çevre, bilgi ve iletişim teknolojilerinin kullanımının artırılmasıyla, çevre korumasında, mekânsal planlamada ve doğal kaynakların sürdürülebilir kullanımında kamunun katılımını içermektedir. Bilgi ve iletişim teknolojilerinin kullanımıyla kamunun katılımının geliştirilmesi çevresel sorunlarla ilgili konularda demokratik yönetişimi de iyileştirecektir.

E-demokrasi aslında demokrasinin geleneksel işleyişinin bir tamamlayıcısı konumundadır. Bilgi toplumunun da ayrılmaz bir parçasıdır. Geleneksel süreç e-demokrasinin araçlarıyla daha etkin bir şekilde kullanılmış olacaktır. E-demokrasi karar alıcılardan vatandaşlara kadar tüm paydaşlara tanıştırılmalıdır. E-demokrasiye katılımın sağlanması eğitimi ve pratikleri gerektirmektedir. Paydaşlara e-araçların nasıl kullanılabileceklerini öğrenme konusunda ayrıca özel bir çaba harcanmasını da gerektirmektedir."

Avrupa Konseyince geliştirilen E-demokrasi temelli belirtilen ön çalışmalarda yukarıda belirtilen temel fikirler, E-devlet için hemen hemen ayni mantıksal çerçevede değerlendirilmiştir. E-devlet; tüm vatandaşlar ve iş dünyasına; sınırsız, kişiselleştirilmiş, kullanıcı dostu, uçtan uca dijital kamu hizmetleri sunulmasını sağlayan temel yaklaşımdır. Yenilikçi gelişmeler, vatandaşların ve işyerlerinin ihtiyaçları ve talepleri doğrultusunda daha iyi hizmetler tasarlamak ve sunmak için kullanılmaktadır. Kamu idarelerinin de kendi paydaşlarıyla ve birbirleriyle olan hizmet etkileşimlerini kolaylaştırmak için yeni dijital ortamın sunduğu fırsatları kullanması önem taşımaktadır.

ETKİNLİK ARACI OLARAK KAMU YÖNETİMİNİN BİLİŞİM-İLETİŞİM TEKNOLOJİLERİYLE MODERNİZASYONU (MALMÖ DEKLARASYONU)

2009 yılında gerçekleştirilen Malmö Deklarasyonu (European Union, 2009, s. 4,5) Avrupa İdareleri için aşağıda yer alan temel ilkeleri 2015 yılına kadar gerçekleşmesi için hedef olarak belirlemiştir. Bu ilkeler;

- Kullanıcıların ihtiyaçlarına göre tasarlanan ve üçüncü taraflarla işbirliği içinde geliştirilen kamu hizmetlerinin yanı sıra, kamusal bilgiye erişimin, izlenebilirliğin artırılması ve etkin katılımın sağlanması için etkili kullanımının vatandaşlar ile kurum ve kuruluşların hizmetine verilmesi,
- Avrupa Birliğinin herhangi bir yerinde okumak, çalışmak, ikamet etmek ve emekliye ayrılmak gibi, dolaşım ortaklığına hizmet edecek şekilde kusursuz e-Devlet hizmetlerinin yerine getirilmesi,
- Yönetimin yükünü azaltmak, etkinlik ve etkililiği artırmak için kurumsal süreçleri geliştirmek ve sürdürülebilirliği teşvik etmeye hizmet edecek e-Devlet mekanizmalarının kullanılması, bu tercih sürdürülebilir düşük karbon ekonomisini de geliştireceği,
- Politika gereklerinin yerine getirilmesi için uygun stratejik unsurların tesis edilmesinin, gerekli, yasal ve teknik ön koşulların oluşturulması ile mümkün olabileceğidir.

Hükümetler maliyetleri düşürerek, daha az kaynakla daha iyi kamu hizmetleri sağlamayı hedeflemek zorundadır. Bu yukarıda sayılan siyasi önceliklerin her biri, daha iyi kamu hizmeti sağlamaya yönelik olup, vatandaşlarla etkileşim için de daha iyi fırsatlar oluşturmaktadır. Hizmet odaklı yenilikçi teknolojiler de özellikle dijital ortamlarda daha iyi imkânlar yaratabilmektedir. E-devlet uygulamaları sayesinde modern ve verimli çalışması beklenen kamu yönetimlerinin, tam da kendilerinden beklendiği gibi, halka ve iş ortamına, hızlı ve kaliteli hizmet sağlamaları gerekmektedir. Kamu idarelerinin hizmetleri yürütürken günün ihtiyaçlarına uygun hale getirmeleri, mevcut süreçlerin ve hizmetlerin raf ömrünü ya da geçerliliklerini yeniden düşünmeleri ve tasarlamaları, verimliliğin yaygınlaşması için oluşturulmuş veri ve hizmetlerin, diğer kurum ve kuruluşlara ve sivil toplumun kullanımlarına açmaları gerekmektedir.

Belirtilen bu çabaların gerçekleşmesi için, anahtar dijital sağlayıcılara güvenilmesi gerekmektedir. Dijital kamu hizmetlerin geliştirilmesine ilişkin

maliyetlerin düşürülmesi önem taşımaktadır. Yine uygulamayı hızla sağlayabilmek ve kurumsal-toplumsal birlikte çalışabilirliği artırmak için, çalışmalar, paydaşlarca kabul edilmiş standartlara ve teknik şartnamelere dayalı olarak kullanılabilecek şekilde paylaşılmalıdır.

Devlet yönetiminin temel çalışmaları da e-devlet felsefesi içinde geliştirilmektedir. Kamu idarelerinin e-ihale, sözleşme kayıtlarının kullanımı ve birlikte çalışabilir e-imzalara geçişine destek vermek için çalışmalar Türkiye'de devam etmektedir. İdarenin zorlamasından çok, halkın da bu yeniliklere açık olması ve desteklemesi önem taşımaktadır. Bu nedenle de önce kamu idaresinin güvenirliği sağlaması gerekmektedir. **Kamu yönetiminde, çoğu kere hantal işleyiş yapısı ve bürokratik zihniyetin baştan aşağı değişmesi, yeni masraflar ve ek vergiler anlamına gelmektedir.**

Kamu hizmetlerinin verimli görülmesi, iş hayatının işleyişinin verimliliğini sağlayacak elektronik işlemlerde, elektronik kimlik ve güven hizmetlerinden yararlanmayı hızlandırmak için bireylerin ve idarelerin çaba göstermeleri gerekmektedir. Dijital kimlikli işletmelerde (örneğin e-imza, web sitesi kimlik doğrulaması), mobil kimlik ve güvenliği sağlayıcı hizmetler de dâhil olmak üzere, elektronik kimlik (e-kimlik) sınır ötesi ve sektörler arası kullanımını hızlandırmak için yapılacak diğer eylemler (örneğin; bankacılık, finans, e-ticaret) ve kamu sektöründe, e-adalet gibi çalışmalar gerekli adımlar olarak öne çıkmaktadır. Bu çalışmalar büyük ölçekli hizmetlerdir. Oysaki hayatın akışı içinde küçük ölçekli alışveriş ve hizmetlerde de "güvenli kimlik doğrulama" ve "ürün güvenliği doğrulama" gibi birçok yönde çeşitli dijital kullanımı sağlama ve kolaylaştırma ihtiyacı ortaya çıkmaktadır. Bu çalışmalar, önemli bir kamuoyu araştırmasına ihtiyaç göstermektedir. E-devlet çalışmalarından olan, e-kimlik, e-imza hatta e-tanımlanmış ses gibi konular üzerinde çalışmak stratejik bir öneme sahiptir ve doğrudan kimlik güvenliği ile ilgilidir.

Ayrıca, "Güvenilirlik ve Güvenlik" ilkesine uygun olarak, kamu sektörüne ilişkin veriler ve hizmetler üçüncü tarafların kullanımına açılmakta ve yeniden kullanımları kolaylaştırılarak, kamu idarelerinden, kapasite artışı, büyüme ve iş imkânları yaratabilecek yeni fırsatlar geliştirmeleri beklenmektedir. Başka bir ifadeyle belirtilen veri paylaşımının kamu yönetiminin halka yakınlaşması, daha şeffaf ve sorumlu bir yönetim haline gelerek demokratikleşeceği öngörüsü ortaya konulmaktadır (Council of Europe, 2009, s. 9).

E-Devlet olarak, alışılagelen çeşitli kamu idaresinin işleyişine yönelik konularda vatandaşın yüksek hizmet kalitesi beklentisi artmaktadır. Mülkiyet edinmede sorun yaratan yanıltıcı emlak bilgilendirmelerinin önüne geçecek, halka güven veren özellikle arazi/mekâna ilişkin güvenilir kamu verilerine erişmeye yönelik konularda, halkın istek göstereceğini beklemek gerçekçi olacaktır. Kentsel arazi kullanımı, trafik planlaması ve bilimsel amaçlar için mekânsal verilerin kullanımı, doğal çevre üzerindeki olumsuz etkilerin tespiti ve azaltılması gibi toplumsal ihtiyaçlara cevap veren yeni girişimlerin gerçekleşebileceğini düşünmek mümkündür. Bilimsel verilere ve mülkiyet haklarına dayalı, kent ve kır planlaması ve politika yapısını geliştirecek, afetlere karşı güven sağlayan yüksek kaliteli mekânsal verilerin (örneğin kadastrolar, haritalar, adresler, binalar, parklar, korunan alanlar, doğal risk alanları, vb.) kayıtlarının tutulmasına duyulan ihtiyaç e-devlet süreçlerini destekleyecektir.

Ulusal E-Devlet stratejilerinden sorumlu kurum ve kuruluşların belirlenmesi için bir "e-Devlet Eylem Planı Yönetim Kurulu" benzeri kurullar oluşturulması önem taşımaktadır. Aslında kamu, özel ve sivil ortaklı temsilcilerden oluşturulmuş bir strateji üreten Yürütme Kurulunun, planlamadan kontrole kadar olan bütün süreci iyi tanımlanmış bir Eylem Planı oluşturması önem taşımaktadır. Kuşkusuz söz konusu, E-Devlet Eylem Planı'nda önerilen tedbirlerin sunulması, ancak ortak bir taahhüt ve çok ortaklı katılımcı anlayışla mümkün olacağı öngörülmektedir.

E-DEVLET ÇALIŞMALARININ TEMEL İLKELERİ

E-devlet çalışmalarına destek verecek eylem planının tamamlayıcı bir parçası olarak başlatılacak olan girişimler, paydaşlar tarafından güçlü bir şekilde desteklenmesi gereken aşağıdaki temel ilkelere uymalıdır (European Union, 2016, s. 3).

Dijital yapıyı oluşturmak: Kamu idareleri, hizmetleri (makine tarafından okunabilir bilgiler dâhil), dijital tercih edilen seçenek olarak sunmalıdır. Diğer hizmet kanalları, herhangi bir beklenmeyen durum için kullanıcıların istifadesine sunulmak üzere kullanılabilir halde tutulmalıdır. Ayrıca, kamu hizmetleri tek bir irtibat noktasından ve çeşitli iletişim kanallarından yürütülmelidir.

İlkesel teklik: Kamu idareleri vatandaşların ve iş hayatının, aynı bilgiyi yalnızca bir kamu idaresinin sağladığından emin olmalıdır.

Kapsayıcılık ve erişilebilirlik: Kamu idareleri, çok geniş bir kapsam içeren, çocuklar, gençler, yaşlılar ve engelli bireyler gibi farklı ihtiyaçlara hitap eden dijital kamu hizmetlerini tasarlamalıdır.

Açıklık ve şeffaflık: Kamu idareleri kendi aralarında bilgi ve veri paylaşmalı ve vatandaşların ve işletmelerin kendi bilgilerine erişerek kontrol etmeleri, güncellemeleri ve gerekirse kendi verilerini düzeltmeleri sağlamalıdır. Kullanıcıların, iç ve dış paydaşlarını da kendilerine yönelik idari süreçleri izleme ve katılım ile katkılarına açmalıdır.

Sınırötesi çalışmalar: Kamu idareleri, ilgili dijital kamu hizmetlerini sınırların ötesine uygun hale getirerek, sınır dışında ve sınır içinde hizmetlerin erişimlerinde ayni etkinlik ve verimliliği sağlamalıdır.

Birlikte çalışabilirlik: Hangi verilerin paylaşılabileceği belirlenerek, verilerin ve dijital hizmetlerin erişilebilirliğini sağlama ve sorunsuz çalışacak şekilde tasarlamalıdır.

Güvenilirlik ve güvenlik: Bahse konu olan bütün bu çalışmaların unsurlarının, tasarım aşamasında bütünleştirerek kişisel veri koruma ve gizlilik ve Bilişim İletişim Teknolojilerinin(BİT) güvenliği hakkındaki yasal çerçeveye uydurulması hatta daha iyi hale getirilmesi sağlanmalıdır.

E-devlet etkinliği için listelenen bu konular, ister bir merkezden veya çok farklı kanallardan dağıtılsın, dijital hizmetlere olan güvenin artması ve bilgilerin tam bir sorumluluk içinde kullanılması için uyulması gereken önemli ön koşullardır. Kamu Yönetimlerinin, dijital dönüşümünü hızlandırmak için gerekli politika önceliklerinde 3 temel yaklaşım öngörülmektedir. Bunlar, i) kamu yönetimini modernize etmek, ii)

sınır ötesi kurumsal işbirliğinde işlerlik sağlamak ve iii) kurumların halkla kolay etkileşimini sağlamak amaçlı stratejik hedefler oluşturmaktır.

Sosyal ağlar gibi yenilikçi teknolojilerin mevcudiyeti, iletişim becerisini de artırmıştır. Özellikle genç yaş grubu iletişim teknolojilerini kullanmada daha etkin görünmektedir. Kuşkusuz teknoloji kullanımına ilişkin kapasite artışı, her türlü hizmete erişimi kolaylaştırırken, halkın bir bütün olarak beklentilerini de artırmaktadır. Ancak herkes hemen her konuda e-devletin sağladığı imkânları kullanma konusunda, yeni bir beceri istediği için veya güvenlik riski açısından (e-imza vb) istekli olmayabilir. Yeni teknolojilerin getirdiği kamu hizmeti erişim kolaylıkları yanı sıra şartnamelerinin de halk yararına özenle düzenlenmesi vatandaşların da memnuniyetini sağlayan bir toplumsal ortam yaratabilir. İdarelerin, daha az kaynakla daha fazla hizmet sunması için BİT teknolojilerini kullanması önem taşımaktadır (European Union, 2010, s. 3-11) Belirtilen bu politika önceliklerinin yerine getirilmesi amacıyla oluşturulması gereken eylem planlarının somut olarak çevrimiçi kamu hizmetleriyle ilgili olarak ele alınması gerekmektedir.

E-Devlet'te işbirliğini desteklemek için ekonomi-politikası temel ilkeleri açısından önemli nedenler bulunmaktadır. E-Devletle ilgili ortaklaştırılan çalışmaların temel dayanağı, kamu kaynaklarının verimli kullanılmasını sağlayarak kamu harcamalarını azaltmaktır.

E-DEVLET VE KULLANICI KOLAYLIKLARI

E-devlet çalışmaları birçok kullanıcı kolaylıklarına da hizmet etmektedir. Aşağıda bu konuya yer verilmektedir.

Kullanıcının Yetkilendirilmesi

E-devlet konusunda kullanıcıların kapasitesinin, kamuoyuna açık bilgilere kolaylıkla erişimi ve karar verme süreçlerine etkin katılımının sağlanacak şekilde güçlendirilmesi de gerekmektedir. Gelirlerin tahsilâtını takip etmek, izlemek, okullara veya üniversitelere kaydolmak, çevrimiçi kimlik talep etmek ve almak, çevrimiçi vergi beyannameleri göndermek gibi hizmetler gelişen e-devlet hizmetleridir. Ayrıca, e-devlet hizmetlerinin kullanılabilirliği ve e-devlet hizmetlerinin (İnternet, TV, telefon, mobil cihazlar veya uygun olduğunda aracılar aracılığıyla) birden fazla kanal üzerinden geliştirilmesi önerilmektedir.

Kamu sektörü sahip olduğu bilgi birikimi nedeniyle bir altın madenine benzetilmektedir. Aslında, kamu yöneticilerinin yetkisiyle topladığı verilerin çoğu, yalnızca sınırlı kişisel veriler(sertifika alımı) ve vatandaşların yükümlülüklerine yönelik(vergi ödeme) benzeri bir amaç için kullanılmamaktadır. Özellikle kişisel olmayan, toplumu ilgilendiren verilerin (coğrafi, demografik, istatistiksel, çevresel veriler, afetlerde erken uyarı vb.), iletişim araçları vasıtasıyla erişilebilir bir yapısallıkta sunulması, vatandaşların ve işletmelerin çalışmalarını geliştirecek yeni yöntemler geliştirilmesi ve bağlantılı olarak yeni ürün ve hizmetler sağlanması beklenmektedir. Kuşkusuz e-devlet hizmetleri, ister yurt içi kamu hizmetlerinde olsun, isterse yurtdışındaki vatandaşları için planlansın, **e-adalet, e-çevre, e-afet** vb çeşitli alanlarda öncelikle kullanım güvenliğinin sağlanması önem taşımaktadır.

E-Vatandaş/E-Hemşeri ve E-Devlet Karşılıklı Sorumluluklar

Kamu hizmetleri artan oranda dijitalleşmekte ve çevrimiçi olarak erişilebilir hale gelmektedir. Vatandaşların beklentisinin ne olduğu ve tatmini, ilkelerin netleştirilmesi, vatandaşların ve devletin karşılıklı sorumluluklarına ilişkin dijital devlet-vatandaş arasındaki sözleşmenin tesisi konuları da demokratiklik ve sürdürülebilirlik açısından önem taşımaktadır (European Public Administration Network, 2008).

Bir idari birim, yürüttüğü hizmete yönelik olarak, vatandaşa ve girişimcilere teminat vermelidir. Teminata ilişkin beyanlar, aynı zamanda hizmet standartları olarak da adlandırılmaktadır. Bu standartların ne olduğunu bilen hizmet alanlar, hizmetten ne beklediklerini bilirler ve aksaması veya standardın sağlanmaması bağlamında yönetimi sorgulayabilirler. Başka bir ifadeyle "**vatandaş sözleşmesi**" hizmetin etkinliğini sağlamada, idari açıdan iyi bir uyarıcıdır. Hizmet standartları, ödeme süreleri, kalite derecesi ve güler yüzlü hizmet gibi hizmetin yönetim süreciyle ilgilidir. Vatandaş Sözleşmesi, i) vatandaş odaklı hizmet standartları, ii) iletişim, iii) tazminat olmak üzere üç unsura sahiptir.

Vatandaş Sözleşmesi uygulamasıyla, bir kuruluşta kamu hizmetinin kalitesinin iyileştirilmesine yol açan dinamizmi oluşturmak hedeflenmektedir. Bu bağlamda, vatandaş katılımını büyütmek, hizmetten yararlanan memnuniyetini arttırmak, personel memnuniyetini arttırmak, şikâyetlerin ele alınmasını iyileştirmek gibi sonuçlar beklenmektedir. Bu konular personel açısından kurumsal sadakat, kullanan açısından güven ve politik yabancılaşmama kavramlarıyla yakından ilişkilidir. İdarenin ilkesel sorumluluklarını ortaya koyan bir düzenleme örneği aşağıda yer almaktadır.

Hollanda Devletinin, vatandaşa karşı sorumluluğunu ortaya koyan, E-Vatandaş Kalite Şartları İlkeleri: (United Nations Public Administration Network, 2018)

1. İletişim kanalları seçimi: Sayaç, mektup, telefon, e-posta, internet kullanımı sağlanır.

2. Şeffaf Kamu Sektörü: Vatandaşlar resmi bilgi edinmek için nereye başvuracaklarını bilir.

3. Hak ve Görevlere Genel Bakış: Vatandaşların hak ve görevleri açıkça bilinir.

4. Kişisel Bilgi Hizmeti: Özel bilgi, kişisel internet sitesi mevcuttur.

5. Uygun Hizmetler: Vatandaşlar sadece bir kez sunumu olan, proaktif olarak kişisel bilgi verir.

6. İzlenebilir Süreçler: İdari süreçlerin açıklığı ve şeffaflığı sağlanır.

7. Dijital Güvenilirlik: Güvenli kimlik yönetimi uygulanır ve elektronik belgeler güvenli şekilde saklanır.

8. Öğrenen Yönetim: İdare, hataları telafi eder ve öğrenir.

9. Sorumlu Yönetim: Vatandaşlar hizmeti karşılaştırarak hizmeti değerlendirir ve idareyi kontrol eder.

10. Katılım ve Yetkilendirme: İdare, vatandaşların katılımını ve idareye katkılarını teşvik eder ve vatandaş memnuniyetini sağlar.

Vatandaş açısından da, e-devletin kontrolündeki sorgulamalar kalite şartı ile bağlantılı olup hakları aşağıda listelenmiştir: (United Nations Economic Commission for Europe, 2018, s. 3)

1. İletişim Kanalının Seçimi: Bir vatandaş olarak, idare ile hangi yolla etkileşimde bulunacağımı kendim seçebilirim. İdare; sayaç, mektup, telefon, e-posta, internet gibi çok kanallı hizmet sunumunu, yani kullanılabilirliği sağlar.

2. Şeffaf Kamu Sektörü: Bir vatandaş olarak kamu hizmetlerine yönelik resmi bilgiler için nereye başvurulacağını biliyorum. İdare, tek elden-hizmet teslimatını garanti eder ve yanlış kapılara yönlendirmez, kusursuz davranır.

3. Hak ve Görevlere Genel Bakış: Bir vatandaş olarak hangi hak ve sorumluluklara sahip olduğumu biliyorum. İdare, haklarımın ve görevlerimin hepsinin yerine getirilmesini açıklık ilkesi içinde sağlar.

4. Kişiselleştirilmiş Bilgiler: Bir vatandaş olarak, güncel ve tutarlı eksiksiz bilgi almaya hakkım vardır. İdare, ihtiyaçlarıma göre uyarlanan uygun bilgiyi sağlar.

5. Uygun Hizmetler: Bir vatandaş olarak, proaktif bir şekilde sunulacak kişisel verileri bir kez vermeyi seçebilirim. İdare kaydettiği verileri açıklar, rızam olmadan veri kullanmayarak beni korur.

6. Kapsamlı Prosedürler: Bir vatandaş olarak idarenin nasıl çalıştığını ve süreci yönettiğini kolayca öğrenebilirim. Yönetim beni, izleme yoluyla dâhil ettiği süreçlerden haberdar eder.

7. Güven ve Güvenilirlik: Bir vatandaş olarak idarenin elektronik olarak yetkin olduğunu kabul ediyorum. Güvenli kimlik yönetimini ve elektronik belgeleri güvenilir depolamayı garanti eder.

8. Vatandaşı Düşünen İdare: Bir vatandaş olarak iyileştirme için fikirler yazabilirim ve şikâyet ederek bilgilendiririm. İdare hataları telafi eder, hizmet ve süreçlerini geliştirmek için geri bildirim kullanır.

9. Sorumluluk ve Kıyaslama: Bir vatandaş olarak yönetimin çıktılarını ölçebiliyorum, kontrol edebiliyorum ve kıyaslayabiliyorum. İdare, performansına ilişkin kıyaslama bilgilerini aktif olarak tedarik eder.

10. Katılım ve Güçlendirme: Vatandaş olarak çıkarlarımı bilme ve karar verme sürecine katılıma davet edildim. İdare bu yetkilendirmeyi destekler ve gerekli bilgi ve araçların mevcut olmasını sağlar.

E-Devlet çalışmalarının sürdürülebilirliği için yönetimler, eğitim kurumları ve sivil toplum örgütlerinden 400'den fazla temsilci, 20–22 Haziran 2017 tarihlerinde Strazburg'da düzenlenen önemli bir konferansta Avrupa'daki vatandaşlık ve insan hakları eğitiminin geleceğini tartışmıştır (Council of Europe, 2010)

Günümüzde Avrupa'da demokrasi ve insan haklarına yönelik ciddi sorunlar olduğu, özellikle Avrupa Birliği toplumlarında dışlama, ayrımcılık ve kutuplaşma,

popülist milliyetçi söylemlerin artan oranda kullanımına ilişkin kaygılar ifade edilerek, geleneksel demokratik süreçlerde hayal kırıklığı yaratan gerileme, terörizm ve şiddet yanlı aşırı hareketlerin yükselişi, göçmen ve mültecilerin topluma uyumuna ilişkin engellerin varlığı ve yavaş ilerleme temel tartışma konuları olarak öne çıkmıştır. Avrupa Müktesebatının zengin birikiminden yararlanılarak, toplumların demokratik gelişmelerini sağlayacak, demokratik kültürü geliştirecek, sürdürülebilir kalkınma için eğitime önem vermek ve çok çeşitli aktörlerden(yönetişim) destek almak hedefleri tartışılarak kayda alınmıştır.

Avrupa Birliği yıllar itibariyle terör ve terörün geldiği duruma yönelik tespitlerini ortaya koyan raporlar hazırlamaktadır. 2018 tarihli Rapora göre (EUROPOL, 2018, s. 15), Terörist grupların interneti, takipçilerine ulaşmak ve mesajlarını yaymak için kullandıkları tespit edilmiştir. Siber teröristlerin özellikle zarar vermek için istihbarat toplama, enerji endüstrisi ve güç şebekelerine saldırma planları yapma doğrultusunda becerilerini artırmaya çalıştıkları ve bu nedenle yine internet imkânlarından yararlandıkları tespiti yapılmaktadır. İnsanlık tarihi boyunca bilinen hırsızlık başta olmak üzere çeşitli suçlar artık internet aracılığıyla yapılmaktadır. İnternet ortamını kullanımıyla ortaya çıkan siber suçların iki yönde artacağı öngörülmektedir. İlki doğrudan devletlere yönelen klasik saldırılar (real world attack), diğeri de karma saldırılar (hybrid attack) olup bu saldırıların acil durumlar ve kamu hizmetlerin düzenli işleyişini bozmaya yönelik gerçekleşebileceğine ilişkin öngörüler yer almaktadır. İnternet iletişimi sayesinde, saldırıları anlık gösteren, siber saldırı haritalarında ülkelerarası e-hareketliliği görmek mümkündür. Bahse konu olan bu gözlemler güvenlik konusundaki kamu gayretinin önemini ortaya koymaktadır.

Siber Saldırılar Ulusal Mevzuatı Oluşturma Gerekliliği

Günümüz dijital dünyasında devlet yönetimlerinin, ülke vatandaşları başta olmak üzere, ülkede yaşayanları korumak için idari yapılanmaları gözden geçirmesi önem taşımaktadır. (Dahora, 2011, s. 240-243) Bu konuda süreç içinde hızla hareket eden kurumsal–teorik iyi bir örnek olarak Amerika Birleşik Devletleri tecrübesi aşağıda yer almaktadır (Chief Information Officer).

Amerikan halkını dijital dünyanın tehditlerinden korumak için Kongre ile birlikte çalışarak, 2015 Güvenlik Yasası olarak adlandırılan bir düzenleme yapılmıştır. Bu çalışma 2000'li yılların başında geliştirilen uygulama yöntemlerinin (policy) geliştirilmiş halidir. Bu sayede özellikle uluslar arası şirketlerin siber güvenliğini güçlendirmek için önemli araçlar sağlanmıştır. Bu çalışmalarda dikkati çeken husus, Amerikan yönetiminin marketten herhangi bir gündelik ihtiyaç için ürün satın almaktan ticari ve sanayi faaliyetlere kadar, üretici ve tüketicinin güvenliğinin sağlanması için kamu yönetiminin baştan aşağı yenilenmesi ve yeni yatırımların yapılmasının önemli adımlarının atılacağının ve atıldığına ilişkin gelişmeleri kamuoyu ile paylaşan bir dizi çalışmalar ile ilgili idari ve mali bilgilerin verilmesidir. Bu çalışmalar sürekli güncelleştirilmektedir.

"Günümüz dijital dünyasında Amerikalıları korumak için cesur adımlar atmak" gerekliliği diye başlayan kamuoyu bildirgelerinde, idari çalışmaların önemi vurgulanmaktadır. Genel olarak, bu idari bilgilendirmelerde, ticari faaliyetlerin yönetiminden, arkadaşlarla iletişim kurmaktan, yol tarifine kadar çevrimiçi bir

dünyanın günlük yaşantıyı etkilediği ve yeniden biçimlendirdiği konusunun farkındalığının sağlanmasına vurgu yapılmaktadır. Siber güvenlik işgücünü geliştirmek ve korumak konunun can alıcı önemli hususlarından birisidir. Ayrıca mevcut, yeni ve gelişmekte olan teknolojinin en iyisini kullanmak için kamu ve özel sektör araştırma ve geliştirme toplulukları ile birlikte çalışmak da dikkate alınmalıdır. Kritik siber güvenlik boşluklarını ve ortaya çıkan öncelikleri tespit ederek boşlukları ortadan kaldırmak için öncelikli eylem planlarını oluşturmak önem taşımaktadır.

Sürekli gelişen dijital çağ; kamu ekonomisi, işletmeler, eğitimde vb kamusal hizmetlerde sınırsız fırsatlar sunmakla birlikte, adapte olmayı gerektiren yeni nesil tehditleri de ortaya çıkarmıştır. Suçlular, teröristler ve ülke yönetimini ile insanlarını incitmek isteyen ülkelerin varlığına işaret edilerek, bir ülkeye yapılan doğrudan klasik saldırmadan, çevrim içi saldırıların daha kolay ve etkili olduğuna ve sistematik kriz yarattığına işaret edilmektedir. Amerika'da en hızlı büyüyen suç kimlik hırsızlığı olup, film endüstrisinin popüler konusudur. Özetle, Amerikan Başkanı, dijital çağda güvenlik konusuna önem verileceğine ve Amerikan halkına güvenlik yaklaşımının cesurca yeniden değerlendirileceğine işaret etmektedir. Başkan, yönetimine kısa vadeli önlemleri alan ve siber güvenlik bilinci ve korumalarını artırmak, gizliliği korumak, kamu güvenliğini sağlamak için uzun vadeli bir strateji yürürlüğe koyan bir Cybersecurity Ulusal Eylem Planı (CNAP) uygulamaktadır.

Türkiye'nin de, Cumhurbaşkanının sorumluluğunda yapılanmış, Ulusal Siber Güvenlik Stratejisi, Eylem Planı (T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016) hazırlanmıştır. "*Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması*" (4.2) değerlendirmesi Eylem Planında yer almaktadır. Siber Planda, yukarıda yer alan uluslar arası gelişmeler ve bilgi içeriğine uygun olarak siber temel ilkelerine yer verdiği görülmektedir.

20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi Ulaştırma ve Altyapı Bakanlığına verilmiştir.

Siber uzay, ulusal siber uzay, kritik hizmet ve kritik altyapı gibi yeni kavramlar ve sorumluluklar listesi literatüre girmiştir. Temel olarak, can kaybına, büyük ölçekli ekonomik zarara ve ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek hizmetler kritik hizmet ve kritik altyapı kabul edilerek hizmetin yapılmaması ile altyapının çökmesinin önüne geçmek hedeflenmektedir. Siber Güvenlik Ekosistem terimi, mevcut dokümanlarda tanımlanmamakla beraber kavramsal olarak eylem planında yer almaktadır. Bu başlık altında, "stratejik eylem kapsamında kamu, özel sektör, STK ve diğer paydaşların koordineli katkısıyla mevzuattan teknolojiye kadar gereksinimlerin belirlenmesine ve uygulamaya dökülmesine yönelik eylemlerin gerçekleştirilmesi planlanmaktadır" bilgisi yer almaktadır. Siber güvenlik ekosistem konusu temel unsurları itibariyle aşağıda yer almaktadır.

Siber uzay ilk insan yapımı ortam olarak kabul edilmektedir. Diğer doğal ortamlarda olduğu gibi kontrol edilememe özelliği taşımaktadır. Yazılımın içsel ve

bölünmez bir yapıya dönüştüğü siber uzay unsurlar sürekli gelişmekte ve yaşamda giderek artan bağımlılık haline gelmektedir. Bu alan içinde yer alan aktörler (kamu kurum ve kuruluşları, özel şirketler, kar amacı gütmeyen kuruluşlar, bireyler) olup, savunmasız olabildikleri gibi sorun kaynağı da olabilirler. Bu nedenle de güvenilir bir siber ortam (Siber Güvenlik Ekosistem) kurma gerekliliği ortaya çıkmıştır.

Siber Güvenlik Ekosistem uzay, tıpkı doğal ekosistemler benzeri katılımcılara sahiptir. Bu katılım ağında canlı yapılar kadar, siber cihazlarda farklı bir çeşitlilik katmaktadır. Belirtilen bu unsurlar, çok amaçlı etkileşim içinde de olabilirler. Siber uzayda dağılmış ve ulusal sınırları aşan bu sistem bütününde bilgi güvenliğini sağlayacak donanım ve yazılım satıcıları, uzman dijital personel ve danışman, bilgisayar korsanları (hacker), standardizasyon ajansları, akreditasyon ve eğitim yapılanmaları ve farkındalık sağlayacak akademik konferanslar ve araştırma makalelerinin yayımlanması önem taşımaktadır.

Siber suçlara karşı eğitimli personelin güçlendirilmesiyle de bağlantılı teknik altyapının sürekli gözden geçirilerek işlevselliğinin artırılması; özel amaçlı teşkilatlanma yanında, Cumhurbaşkanı tarafından dijital suçlar, Türkiye Cumhuriyeti vatandaşlarına hitaben siber saldırıları önleyici çalışmalarda bulunan e- güvenlik taahhüdü olarak "Siber Güvence Beyanının" oluşturulması; Türkiye Cumhuriyeti Cumhurbaşkanının siber saldırılara yönelik çok yönlü sorumluluğunu ve eylem planlarını ortaya koyan bir ulusal bildirge yayınlanması yerinde olacaktır. Eylem planlarında hükümetin, şirketlerin ve bireylerin birlikteliği, sorumluluğunun belirlenmesi önemlidir. Türkiye'nin Ulusal Siber Güvenlik Stratejisi Eylem Planının incelenmesinden böyle bir beyana yer verilmediği görülmektedir.

Bu veya benzeri kamusal projeler için, "Ulusal Siber Güvenliği Geliştirme" ve kamu hizmetlerinin güvenliği için Siber Olaylara Müdahale Ekipleri (SOME) gibi yapılanmaları oluşturmak önemlidir. Cumhurbaşkanlığı Kararnameleri ile belirlenen yeni kamu yönetimi yapılanmasında, Cumhurbaşkanlığı bünyesinde, 1 sayılı Kararname ile oluşturulan merkezi düzeydeki güvenlik yapılarını destekleyen "**Cumhurbaşkanlığı Politika Kurulları**" (CK1,md.20), katılıma önem veren önemli bir etkin yönetim aracıdır. Başka bir ifadeyle bu yapılar yeni yönetim felsefesine uygun olarak katılıma da açık olarak biçimlendirilmiş hizmetlerde etkinliği sağlayacak yönetim yöntemidir. Kuruluş amacı itibariyle, Cumhurbaşkanının kamu politikalarını belirlemesine yardımcı olan, bakanlıklarda geliştirilen politika ve hizmetlerin Cumhurbaşkanlığı bünyesinde izlenmesi, değerlendirilmesi ve alternatif politika üretme misyonunu yerine getiren ve literatürde "Karşı Bürokrasi"[3] olarak tanımlanan yapılarla benzerlik göstermektedir.

Kurul üyeleri, Cumhurbaşkanınca atanan ve en az 3 üyeden oluşan ve bir üyenin başkanvekili olarak Cumhurbaşkanı tarafından görevlendirildiği, bu kurullar aşağıda listelenmiştir. Kurulların birbirleriyle bağlantısı olmakla birlikte,"Güvenlik ve Dış Politikalar Kurulu" konumuzla ilişkilidir.

[3] Karşı bürokrasi fikri, ilk olarak Amerika Birleşik Devletlerinde, Başkan Roosevelt tarafından 1939 yılında kurulmuştur. Başkanın kişisel bürokrasi olup, siyasetçileri desteklemek veya onlara yardım etmek yada resmi bürokrasiye dengeleyici nitelikte görev yapma amacı için tasarlanmıştır.:Bilal Eryılmaz (2018) Kamu Yönetimi, 11. Baskı, s. 15

a) Bilim, Teknoloji ve Yenilik Politikaları Kurulu.

b) Eğitim ve Öğretim Politikaları Kurulu.

c) Ekonomi Politikaları Kurulu.

ç) Güvenlik ve Dış Politikalar Kurulu.

d) Hukuk Politikaları Kurulu.

e) Kültür ve Sanat Politikaları Kurulu.

f) Sağlık ve Gıda Politikaları Kurulu.

g) Sosyal Politikalar Kurulu.

ğ) Yerel Yönetim Politikaları Kurulu.

Güvenlik ve Dış Politikalar Kurulunun görev ve yetkileri içinde (CK1,md.26): siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek ve yine bağlantılı afet ve acil durum halleri, sivil havacılık güvenliği gibi konular yer almaktadır.

Kurul üyelerinin katılımcı yaklaşımla oluşturulacağı belirlenmiştir. Söz konusu kurulun Meclis tarafından belirlenecek parti temsilcileri ve hükümet dışı en önemli ticari ve teknik uzman ile strateji uzmanlarından oluşturulması önemlidir.

İçişleri Bakanlığının hizmet birimleri içinde güvenlik ve strateji önemli bir yapısallık oluşturmaktadır (CK1, md. 256). Bu birimler, İller İdaresi Genel Müdürlüğü, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Personel Genel Müdürlüğü, Hukuk Hizmetleri Genel Müdürlüğü, Teftiş Kurulu Başkanlığı, Strateji Geliştirme Başkanlığı, Kaçakçılık İstihbarat, Harekât ve Bilgi Toplama Dairesi Başkanlığı, Sivil Toplumla İlişkiler Genel Müdürlüğü, Güvenlik ve Acil Durumlar Koordinasyon Merkezi(GAMER), Avrupa Birliği ve Dış İlişkiler Dairesi Başkanlığı, Eğitim Dairesi Başkanlığı, Destek Hizmetleri Dairesi Başkanlığı, Bilgi İşlem Dairesi Başkanlığı, İç Güvenlik Stratejileri Dairesi Başkanlığı, Basın ve Halkla İlişkiler Müşavirliği, Özel Kalem Müdürlüğüdür.

Güvenlikle ilgili kurumsal yapılanmalar, gizlilik kuralları içinde çalışmalı, kamu ve özel sektördeki siber güvenlik düzeyini güçlendirmek için geleceğe yönelik olarak kısa, orta vadede (teknoloji hızla değiştiği için) kamu yönetiminin uygulayacağı, ilkesel ve eylemsel olarak önlemler, konusunda tavsiyede bulunma veya görüş bildirme görevini üstlenmelidir. Bu konular: güvenlik konularının bütün boyutlarında kamu güvenliği ve ekonomik ve ulusal güvenliğin korunması; yeni teknik çözümlerin araştırılması ve geliştirilmesinin teşviki; siber güvenlik teknolojilerinin, politikalarının oluşturulmasını sağlayacak en iyi uygulamalarının geliştirilmesi, kullanımı konusunda merkezi yönetim ve yerel yönetimler ile özel sektör arasındaki ortaklıkların güçlendirilmesine yönelik kapsamlı çalışmalar olarak değerlendirilmektedir. E-devlet çalışmalarının tamamen teknik konulara yönelik olmayıp, ayrıca "demokratik" yönünün de olduğunu hatırda tutmak önem taşımaktadır.

Siber güvenlikle ilgili olarak uluslar arası yaklaşımlar ve öneriler genelde aşağıdaki gibi gelişmektedir.

1) Öncelikli güvenlik tanımlama ve yüksek değeri olan bilginin ve varlıkların korunması,

2) Siber saldırılara karşı zamanında tespit ve hızlı yanıt,

3) Başarılı öğrenilmiş derslerin hızlı çözümlemelerinin göz önünde tutulması,

4) Siber güvenlik gücünü oluşturacak en yüksek nitelikli siber personelin işe alınması ve elde tutulması,

5) Mevcut teknolojinin etkin kullanılması ve teknolojik gelişmelerin takibi.

Sürekli sorgulama yöntemi aşağıda gösterilmektedir. Buna göre;

• Hedefler: "Neye ulaşmamız gerekiyor" sorusuna cevap aramakta ve

• Eylemler: "Bu hedeflere ulaşmak için çabalarımızı nasıl ve nereye odaklıyoruz" hususlarına dikkat edilmesini önermektedir. Kuşkusuz kamu yatırımlarının yenilenmesi, bakımının yapılması, eğitim ve diğer konular bir mali külfet getirmektedir. Konuya ilişkin mali yönetimin açıklıkla halk ile paylaşılması, konuya ilişkin vergilendirme ve şeffaflık içinde yapılan çalışmaların mali dökümünün beyanı, halkın desteği açısından önemlidir. Bilgi Teknolojisi Modernizasyon Fonu gibi, Amerika'da üzerinde çalışılan **Fon** benzeri bir çalışma yapılabilir.

DEĞERLENDİRME

Kamu yönetiminin ulusal ve uluslararası düzeyde farklı hizmetlerinde, devlet sırrı olmayan veri ve hizmetlerin vatandaşın erişimine açılmasının, kamu hizmetlerinin yerine getirilmesinde verimliliği artıracağı, kurumların ve vatandaşların idare ile olan ilişkilerinin kolaylaşacağı ve güven faktörünün karşılıklı artacağı beklenmektedir. Mamafih, klasik yüz yüze yöntemde alışıldığı gibi göz önünde oluşturulan idari kayıt üzerinden çalışma daha güvenli bulunmaktadır. Benzer algının dijital ortam için de oluşması ve şeffaflık beklentisi bulunmaktadır. Bu demokratik mekanizmalar yönteminin kullanılma başarısı bağlamında, kamu idareleri daha güvenilir ve demokratik sorumlu yönetimler olarak, halka daha hesap verebilir hale gelecektir.

Dijital Dünya'nın temel konusu, kişisel verilerin korunması ve gizliliğinde, idarenin tam bir yasal koruma sağlamasıdır. Bir eylem ancak gayrimeşru, evrensel hukuka aykırı ve tutarsız olarak değerlendirildiğinde terör ve gerçekleştiren de "terörist" olarak nitelendirme eğilimi bulunmaktadır. Terörist eylemler, tanımı gereği hedefi sivil halk olan ve devletlere yönelik eylemlerdir. Esasen terörden dijital veya değil devletler doğrudan veya dolaylı etkilenmektedir. Bu nedenle devletler gerek kendisini ve gerekse vatandaşı ile diğer yerleşikleri güvenlik gibi temel bir varlık nedeni ile korumak zorundadır.

Türkiye açısından da, devletin ve vatandaşın hak ve sorumlulukları yönüyle sürdürülen çalışmaların temel ilkelerinin netleştirilmesi ve protokoller oluşturularak merkezi erişime açılması, kamuoyunca bilinirliğinin sağlanması önem taşımaktadır. İnsan hakları ve demokratik kültürünü geliştirecek yaygın eğitim çalışmalarına, gerek beşeri gerekse kurumsal kapasite açısından eğitimin her basamağında önem vermek gerekmektedir. Çalışmaların başarısında katılımcı mekanizmalar çok önemli olup, Cumhurbaşkanlığı Danışma Kurullarının yerel/ulusal toplumsal sermayeden mümkün

olan en çok faydayı sağlayacak şekilde planlanması ve yönetilmesi ve e-katılım ile işlevselliğinin artırılması önem taşımaktadır.

KAYNAKÇA

European Union. (2016, 04 19). *European Union Comission and İt's Priorities.* 04 05, 2018 tarihinde http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-179-EN-F1-1.PDF adresinden alındı.

Afet ve Acil Durum Yönetim Başkanlığı. (2013, 12 01). *Türkiye Afet Müdahale Planı.* 10 01, 2018 tarihinde https://www.afad.gov.tr: https://www.afad.gov.tr/upload/Node/2419/files/Afet_Mud_Pl_ResmiG_20122013.pdf adresinden alındı.

Chief Information Officer. (tarih yok). 04 20, 2016 tarihinde Chief Information Officer Topics : https://www.cio.gov/fed-it-topics/cybersecurity/cybersecurity-national-action-plan adresinden alındı.

Council of Europe. (2009, 02 18). *Council of Europe*. 03 25, 2018 tarihinde https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf adresinden alındı.

Council of Europe. (2010, 05 01). 04 04, 2018 tarihinde Council of Europe What We Do: https://www.coe.int/en/web/edc/charter-on-education-for-democratic-citizenship-and-human-rights-education adresinden alındı.

Dahora, K. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

E-devlet (2019) 15.04.2019 tarihinde https://www.turkiye.gov.tr/bilgilendirme?konu=politikalar, adresinden alındı

Eryılmaz, Bilal. (2018). Kamu Yönetimi, 11. Baskı, 15.

European Public Administration Network. (2008, 09 01). 04 04, 2018 tarihinde European Public Administration Network: http://www.eupan.eu/files/repository/7_steps_EN.pdf adresinden alındı

European Union. (2009, 11 18). 04 06, 2018 tarihinde European Comission: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf adresinden alındı.

European Union. (2010, 12 15). *Comission and İt's Priorities.* 04 06, 2018 tarihinde https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF adresinden alındı.

EUROPOL. (2018, 04 20). 09 28, 2018 tarihinde EUROPOL Activities and Services: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 adresinden alındı.

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016, 08 09). *T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı Ulusal Siber Güvenlik Stratejisi.* 09 28, 2018 tarihinde http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden alındı.

Türkiye Büyük Millet Meclisi md.3 . (2003, 03 01). *Sınıaşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesinin Uygun Bulunduğuna Dair Kanun*. 09 24, 2018 tarihinde Mevzuat Bilgi Sistemi: https://www.tbmm.gov.tr/kanunlar/k4800.html adresinden alındı.

United Nations Economic Commission for Europe. (2018). *United Nations Economic Commission for Europe Documents*. 10 01, 2018 tarihinde http://www.unece.org/fileadmin/DAM/ceci/documents/KBD_Newsletter/Issue_4/Poelmans.pdf adresinden alındı.

United Nations Public Administration Network. (2018). 04 04, 2018 tarihinde http://www.burgerlink.nl/Documenten/englishsite/citizen-charters/citizen-charters.html adresinden alındı.