Amerika Birleşik Devletleri ve Avrupa Birliği Düzenlemeleri ile Karşılaştırmalı Olarak Türkiye'de Siber Güvenlik Düzenlemeleri ve Uygulamaları

Av. Gönenç Gürkaynak
ELİG Lokmanhekim Gürkaynak Ortak Avukat Bürosu, Yönetici Ortak.
gonenc.gurkaynak@elig.com

Özet: Değişen dünyanın ihtiyaçları ile doğru orantılı olarak gelişen teknolojilere ayak uydurmak bir tercihten ziyade zorunluluk teşkil etmektir. Teknolojik gelişmeler, sağladığı sayısız imkânların yanı sıra siber suçların gerçekleşmesi için gerekli olan, teknik bilgi ve beceriye daha az ihtiyaç duyan yeni siber suç türlerinin ortaya çıkmasına sebep olmuştur. Bu nedenle, hem bireylerin hem de devletlerin dijital dünyadaki güvenliğini sağlamak adına, siber suç türlerinin değişen niteliğine uygun, "yeni siber suçlarla mücadele yöntemleri" geliştirmek kaçınılmazdır. Bununla birlikte, Türkiye'nin siber güvenliğe ilişkin düzenlemeleri ve uygulamaları ele alındığında, Amerika Birleşik Devletleri'ne ve Avrupa ülkelerine kıyasla Türkiye'nin siber güvenlik meselesine gösterdiği özen ve hassasiyet bakımından bu ülkeleri birkaç adım geriden takip ettiğini söylemek mümkündür. Bu bildiride, bahsedilen çerçevede, Amerika Birleşik Devletleri ve Avrupa Birliği düzenlemeleri ve uygulamaları ile karşılaştırmalı olarak Türkiye'de siber güvenliğe ilişkin hukuki düzenlemeler, uygulamalar ve önlemler ile bunların yeterlilik seviyesi irdelenecektir.

Anahtar Sözcükler: *Siber Güvenlik, Siber Suç, Avrupa Konseyi Siber Güvenlik Sözleşmesi, TCK.*

Abstract: It is not a preference but a must to keep up with technological developments which goes along with the changing world's need. While providing countless opportunities, these developments minimized the need for technical knowledge and capability to perpetrate a cybercrime and caused new types of cybercrimes to occur. Therefore, for the sake of both individuals and nation's complete safety, the need for developing new way of struggle has been occurred in parallel with the changing shape of cybercrimes. That being said, considering Turkey's regulations and practice on cyber security, it drops behind United States of America and European Union Countries in terms of its sensitivity and prudence on the issue. This assertion scrutinizes cyber security regulations, practice and measures in Turkey along with their sufficiency and insufficiency in comparison with USA's and EU's regulations and practice.

I. GİRİŞ

Değişen dünyanın ihtiyaçları ile doğru orantılı olarak gelişen teknolojilere ayak uydurmak bir tercihten ziyade zorunluluk teşkil etmektir. Teknolojik gelişmeler, sağladığı sayısız imkânların yanı sıra bu siber suçların gerçekleşmesi için gerekli olan teknik bilgi ve beceriye olan ihtiyacı azaltmış yeni siber suç türlerinin ortaya çıkmasına sebep olmuştur. Bu nedenle, hem bireylerin hem de devletlerin dijital dünyadaki güvenliğini sağlamak adına, siber suç türlerinin değişen şekli ile paralel olarak yeni mücadele yöntemleri geliştirmek kaçınılmaz bir ihtiyaçtır. Bununla birlikte, Türkiye'nin gerek siber güvenliğe ilişkin düzenlemeleri, gerek uygulamaları ele alındığında, Amerika Birleşik Devletleri'ne ve Avrupa Birliği'ne kıyasla siber güvenlik meselesine gösterdiği özen ve hassasiyet bakımından Türkiye'nin birkaç adım geriden takip ettiğini söylemek mümkündür.

Siber güvenlik, bilişim sistemlerinin temeli olan "bilgi/veri" üzerinden tanımlanmaktadır. Bu doğrultuda, siber

alanın güvenli olabilmesi için gerekli olan temel unsurlar;

(i) bilginin gizliliğinin sağlanması,
(ii) bilginin bütünlüğünün sağlanması ve
(iii) bilginin erişilebilirliğinin sağlanmasıdır.[1]

Erişilebilirlik ile bilginin gizliliği ve bütünlüğü hususlarıyla çelişebilmektedir. Zira bilginin erişilebilir kılınması sağlanırken, gizliliğinin ve/veya bütünlüğünün sağlanması hususunda başka riskler doğabilecektir. Bu nedenle, erişilebilirliğe ilişkin düzenlemeler, erişilebilirliğe konu bilginin gizliliğini ve bütünlüğünü de korumaya yönelik önlemleri de içermelidir.[2] Bu kapsamda, Türkiye'deki mevcut düzenlemeler ve uygulamalar çerçevesinde, siber güvenliğe ilişkin gerekli önleyici mekanizmaların tam anlamıyla sağlanabildiğini söylemek mümkün olmayacaktır.

II. Türkiye'de Siber Güvenliğe İlişkin Yasal Düzenlemeler ve Mevcut Durum

a. Bilgi Teknolojileri ve İletişim Kurumu'nun Siber Güvenliğe İlişkin Uygulamaları

Ülkemizde siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak Bilgi Teknolojileri ve İletişim Kurumu - Siber Güvenlik Kurulu'nun görevidir.[3]

Siber Güvenlik Kurulu'nun kurulmasını takiben Türkiye'nin mevcut durumu ve diğer dünya ülkelerinin durumu göz önünde bulundurularak, Ulusal Siber Güvenlik Stratejisi ve Eylem Planları oluşturulmaya başlanmıştır. Bu doğrultuda ilk defa 25 Mart 2013 tarihinde Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı kararlaştırılmıştır.

Siber Güvenlik Kurulu tarafından yürütülen siber güvenlik eylem planı özetle aşağıdaki gibidir:

i. Yasal Düzenlemelerin Yapılması
ii. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi
iii. Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması
iv. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi
v. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi
vi. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi
vii. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

2015-2016 yıllarını kapsayacak eylem planına ilişkin çalışmalar Ulaştırma Denizcilik ve Haberleşme Bakanlığı koordinasyonunda sürdürülmektedir.[4] 2015 yılının son çeyreğinde olduğumuz göz önüne alındığında, 2015-2016 yıllarına ilişkin eylem planının hâlihazırda kararlaştırılmış olmaması, Türkiye'nin siber güvenliğin sağlanması hususundaki tedbir ve özen eksikliğine ilişkin önemli bir göstergedir.

b. Türk Ceza Hukuku Mevzuatı

Elektronik ağlar vasıtasıyla işlenen klasik suçlar 5237 Sayılı Türk Ceza Kanunu'nda ("TCK") genellikle bahse konu suçlara ilişkin hükümler için ağırlaştırıcı sebep olarak düzenlenmektedir. Suçun "dijital dünyada" işlenmesi, nitelikli hal olarak kabul edilmektedir. Örneğin; bilişim vasıtalarını kullanarak işlenen

[1] Öğün, Mehmet Nesip, *Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler*
[2] Hekim, Hakan, *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları,* Uluslararası Güvenlik ve Terörizm Dergisi • 2013, 4 (2).
[3] http://www.btk.gov.tr/tr-TR/Sayfalar/SG-Genel-Bilgi

[4] Bu bildiri 5 Ekim 2015 tarihinde tamamlanmıştır.

dolandırıcılık suçu "nitelikli dolandırıcılık", bilişim vasıtalarını kullanarak işlenen hırsızlık suçu ise "nitelikli hırsızlık" olarak değerlendirilmektedir.

Elektronik ağların kullanılması bazı suç tipleri için ağırlaştırıcı sebep olarak öngörülürken, tek başına "elektronik ağlara özgülenmiş suçlar" da TCK kapsamında düzenlenmektedir. Elektronik ağlara özgülenmiş suçlar, TCK'da "Onuncu Bölüm" olarak "Bilişim Alanında Suçlar" başlığı altında ele alınmaktadır. Örneğin, "sisteme girme" ve "sistemi engelleme", "bozma", "verileri yok etme veya değiştirme" hususları TCK kapsamında düzenlenmiştir ve ayrı bir bölüm olarak yaptırıma bağlanmıştır.

TCK elektronik ağlar vasıtasıyla işlenen suçların büyük çoğunluğunu kapsamaktadır. Ancak bahse konu düzenlemeler ile uygulama tam anlamıyla bir bütünlük arz etmemektedir. Örneğin, TCK m. 243 kapsamında "sisteme girme" suçu düzenlenmektedir. Aynı maddede, bir suç olarak sisteme girmenin söz konusu olabilmesi için sisteme girmenin yanında "sistemde kalma" şartı da öngörülmektedir. Kişinin bilişim sistemine haksız erişimden sonra, "orada kalmaya devam etme" fiilini gerçekleştirmesini açıklayan yasal bir düzenleme bulunmamakta birlikte, yargı kararlarında da bu husus açıklığa kavuşturulmamıştır. Aynı hususa ilişkin olarak, Avrupa Konseyi Siber Suç Sözleşmesi'nin "Haksız Erişim" başlıklı 2. Maddesinde; "*Her taraf, iç hukukuna uygun olarak, bir bilişim sistemini tamamına veya bir kısmına kasten ve haksız olarak erişimi ("illegal access"), suç haline getirmek için gerekli görülen kanuni tedbirleri kabul eder"* şeklindedir. TCK kapsamında öngörülen düzenleme ile sistemde kalma fiilinin tespit edilemediği ve salt yetkisiz sisteme erişim hallerinde meydana gelebilecek bilginin gizliliğinin ihlali halleri göz önünde bulundurulmamıştır. Bu eksiklik, siber güvenliğin unsurlarından olan "bilginin gizliliğinin sağlanması" hususunda önemli bir boşluk teşkil etmektedir.

Ayrıca, Türk ceza mevzuatı kapsamında düzenlenen siber güvenlik önlemleri siber güvenlik risklerinin bertaraf edilmesi bakımından da yetersizdir. Özellikle özel şirketler açısından gerekli hassasiyeti taşımamaktadır.

III. ABD'de Siber Güvenlik Uygulamaları

Amerika Birleşik Devletleri 11 Eylül 2003 sonrasında siber ortamın güvenliğinin sağlanması için ulusal stratejisini oluşturmuştur. Teknolojik gelişmelerin önüne geçilemez etkisi ve siber ortamın korunması gerekliliği ilk defa bu strateji kapsamında ele alınmıştır. 2003 yılından bu yana siber güvenlik uygulamaları ve önlemlerine ilişkin olarak değişen Dünya'ya paralel gelişmeler yakalamıştır.

Siber güvenliğin geliştirilmesi ve kamusal hazırlığın ve farkındalığın sağlanması hususunda kamu-özel sektör iş birliği meselesini rızaya bağlı bir yardımlaşma olarak düzenleyerek bu anlamda önemli bir adım atmıştır.

Amerika Birleşik Devletleri'nde siber güvenliğin sağlanmasına ilişkin düzenlemeleri içeren en önemli hukuki düzenleme "Computer Fraud and Abuse" Act ("CFAA") isimli yasadır. CFFA kapsamında, TCK'da problemli olarak gördüğümüz hususların bir kısmı da açıklığa kavuşturulmaktadır. CFFA, bilişim sistemlerine özgü suçların yanında bilişim sistemlerinin vasıta olarak kullanıldığı suçları da ele almaktadır. Bu yönüyle TCK ile benzerlikler içermektedir ayrılmaktadır.

Siber suçların hedef sistemin özelliği bakımından ayrıştırılması, CFFA ile TCK arasındaki en önemli farklılıklardan biridir. CFFA'da "koruma altındaki bilgisayar"

kavramına yer verilmektedir. Yapılan tanıma göre "koruma altındaki bilgisayar":

(i) finansal bir kurum ya da devlet kurumlarına münhasıran kullanılan veya bunlarca dolaylı olarak kullanılıp suç fiilinin bunları etkilediği veya
(ii) ABD dışında da olsa eyaletler arası ya da uluslararası ticaret veya iletişim maksadıyla kullanılan bilgisayar" anlamına gelmektedir. Bazı mahkeme kararlarında ağ üzerinde çalışan her bilgisayar koruma altındaki bilgisayar kavramı kapsamına sokulsa da, kanunun özünde böyle bir ayrıma yer verilmesi önemlidir.

CFAA'yı TCK'dan ayıran diğer bir özellik siber suçları ve öngörülen cezaları failin amacına göre de ayrıştırıyor olmasıdır. Bu doğrultuda, TCK kapsamında da kanunda anılan suçlara verilen cezaların failin amacı ve hedef alınan sistemin hassasiyeti göz önünde bulundurularak yeniden düzenlenmesi uygun olacaktır. Zira bu haliyle TCK casusluk veya terörist eylem amacıyla siber saldırı düzenleyen bir kişiyle, arkadaş grubu içerisinde statü edinmek için siber saldırı düzenleyen kişi arasında bir fark gözetmemektedir.[5]

CFAA, "bilgisayar," "finansal kurum", "zarar", "kayıp" gibi pek çok temel kavramı tanımlayarak uygulamada yoruma açık husus bırakmamayı hedeflemiştir. Bu sayede, siber saldırıların sebep olduğu zarar nispetinde yaptırım öngörülmesi mümkün kılınmıştır. Örneğin, TCK yahut diğer sair mevzuat kapsamında, hasarın herhangi bir karşılığı/tanımı bulunmadığından, çok sayıda insanın etkileneceği bir sisteme yapılan bir saldırıyla küçük bir şirketin internet sayfasına düzenlenen saldırı arasında kanun anlamında farklı bir değerlendirme söz konusu değildir. Ancak, saldırıdan etkilenen sistemin çalışmamasının ya da saldırı neticesinde çalışmasının aksamasının doğurduğu netice hasarın tespit edilebilmesi ve yaptırımların orantılı uygulanabilmesi açısından önem arz etmektedir.

Kişisel verilerin korunmasında meydana gelen siber güvenlik ihlaline ilişkin olarak, pozitif bildirim yükümlülüğü de ilk defa Amerika Birleşik Devletleri'nde uygulama alanı bulmuştur. Pozitif bildirim yükümlülüğü, kişisel verilere ilişkin güvenlik ihlalinin vücut bulması halinde bu güvenlik ihlaline konu verinin bünyesinde bulunduğu kuruma/kuruluşa verinin ilgili bulunduğu kişi/kişilere bildirim yükümlülüğü getirmektedir. ABD'nin 47 eyaletinde "pozitif bildirim yükümlülüğü" uygulanmaktadır.

IV. Avrupa Birliği'nde Siber Güvenlik Uygulamaları

Avrupa Birliği siber güvenlik politikası, aşağıdaki ana prensipleri içermektedir:

(i) temel hakların ve ifade özgürlüğünün güvence altına alınması, kişisel verinin ve özelliğinin korunması,
(ii) İnternet'in herkes tarafından erişilebilir olması,
(iii) Demokratik, verimli ve çok taraflı bir siber güvenlik yönetimi sağlanması,
(iv) siber güvenliğin sağlanmasında herkesin (kurum, kuruluş, birey, kamu veya özel sektör ayırt etmeksizin) yer alması.[6]

[5] Hekim, Hakan, *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları,* Uluslararası Güvenlik ve Terörizm Dergisi 2013, 4 (2).

[6] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Cyber security Strategy of the European Union – An Open, Safe and Secure Cyberspace*", Brussels, 2013.

(i) Temel Hakların Ve İfade Özgürlüğünün Güvence Altına Alınması

Avrupa Birliği siber güvenlik politikası temel hak ve özgürlüklerin güvence altına alınmasını önceliklendirmektedir. Bir başka deyişle, bireylerin haklarının güvence altına alınması hususunda güvenli ağ ve sistemler bir ön şart olarak nitelendirilmektedir. Bu doğrultuda, kişisel veri söz konusu olduğunda, siber güvenlik kapsamında herhangi bir bilgi paylaşımı, kişisel verilerin korunması mevzuatına uygun olarak gerçekleştirilmelidir ve bireylerin bu hususa ilişkin tüm hakları göz önünde bulundurulmalıdır.

(ii) İnternet'in Herkes Tarafından Erişilebilir Olması

Avrupa Birliği siber güvenlik politikası, dijital dünyanın üye devlet vatandaşlarının hayatında ne denli büyük bir alan kapsadığını da irdelemektedir. İnternet'e sınırlı erişim ya da erişimin engellenmesi Avrupa Birliği'nde siber güvenlik politikası kapsamında birey bazında bir olumsuz bir adım olarak değerlendirilmektedir. Özetle, İnternet'in sosyal yaşama adaptasyonu bireylere güvenli bir siber ortam oluşturmak yoluyla sağlanmaya çalışılmaktadır.

(iii) Demokratik, Verimli ve Çok Taraflı Bir Siber Güvenlik Yönetimi Sağlanması

Dijital dünyanın çok oyunculu bir mekanizma olduğunun ve bu oyuncuların tek başlarına ya da konsolide halde siber güvenliğin sağlanması hususunda önem arz ettiğinin Avrupa Birliği siber güvenlik politikası oluşturulurken göz önünde bulundurulan hususlardan olduğunu görüyoruz. Gerçekten de, ticari ve devlete ait olmayan teşebbüsler, İnternet'e sağladıkları kaynaklar ve İnternet'i şekillenmesi açısından önemli katkılar sağlamaktadırlar ve siber ortamın oluşumunda önemli bir yer teşkil etmektedirler. Bu doğrultuda, Avrupa Birliği, mevcut İnternet yönetimindeki tüm oyunculu yönetim yaklaşımını desteklemektedir.

(iv) Siber Güvenliğin Sağlanmasında Herkesin (Kurum, Kuruluş, Birey, Kamu Veya Özel Sektör Ayırt Etmeksizin) Yer Alması

Avrupa Birliği, insan hayatının her noktasındaki hızla artan bilgi ve iletişim teknolojilerine bağlılığı siber güvenlik politikasında zayıf noktalar oluşturan bir unsur olarak kabul etmektedir. Siber güvenlik politikası uygulanırken, bahse konu zayıf noktaların özenle tespit edilmesi, değerlendirilmesi, çözümlenmesi ve mümkünse azaltılması yönünde bir yaklaşım benimsenmiştir. Bu kapsamda, bilgi ve iletişim teknolojilerine bağlı olan tüm öznelerin, kamu otoriteleri, özel sektör ve birey ayrımı güdülmeksizin, kendilerinin ve total siber güvenliğin sağlanması hususunda koordinasyonun sağlanması hedeflenmektedir.

Bu doğrultuda, Avrupa Birliği'nin en güncel siber güvenlik strateji planında önceliklendirilmiş beş husus bulunmaktadır:

- Siber direncin sağlanması
- Siber suçlarda kayda değer bir düşüş yakalamak
- Common Security and Defence Policy (CSDP) kapsamında, siber savunma politikasının ve imkânlarının geliştirilmesi
- Siber güvenlik için endüstriyel ve teknolojik kaynakların geliştirilmesi
- Avrupa Birliği için uyumlu bir uluslararası siber güvenlik politikası oluşturmak ve bu kapsamda Avrupa Birliği'nin ana değerlerinin desteklenmesi

Ek olarak, Avrupa Birliği'nde mevcut en önemli hukuki metin Avrupa Konseyi

Siber Suçlar Sözleşmesi'dir. 2001 yılında kabul edilen, 2004 yılında yürürlüğe giren çok taraflı antlaşmaya Türkiye 10 Kasım 2010 tarihinde taraf olmuştur ancak sözleşme hala Türkiye'de onaylanmamıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi, İnternet ve diğer bilgisayar sistemleri üzerinden işlenen suç türlerini ele alan ilk uluslararası sözleşmedir. Sözleşmenin öncelikli amaçlarından biri sözleşmeye taraf ülkelerin maddi ceza hukuku hükümlerini siber suçlar alanında birbirine paralel uygulamalar haline getirmektir. İkincil amacı ise siber suçlarla mücadeleye ilişkin olarak, hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmaktır.

Avrupa Konseyi Siber Suç Sözleşmesi'ni takiben Avrupa Birliği'nce çerçeve kararlar alınmıştır ve yürürlüğe konmuştur.[7] Bu çerçeve kararlarda Türkiye'nin yerel hukuk sisteminde yapılacak değişikliklerde göz önünde bulundurulmalıdır.[8] Zira Türkiye gibi gelişmekte olan bir ülkenin yerel hukuku da dinamik bir nitelik taşımaktadır.

Son olarak, Amerika Birleşik Devletleri'ndeki düzenlemelerden ve uygulamalardan bahsederken değindiğimiz "pozitif bildirim yükümlülüğü" meselesine Avrupa Birliği açısından da değinmek gerekir. Avrupa Birliği'nde kişisel verilerin korunması ve ihlali halinde pozitif bildirim yükümlülüğü getirildiği haller Kişisel Verilerin Korunması Direktifi uyarınca düzenlenmektedir. Bu direktif uyarınca, veri kontrolörünün veri koruması ihlali olması halinde veri koruma otoritesine bildirim yükümlülüğü söz konusudur. Elektronik Haberleşme Direktifi uyarınca ise, hizmet sağlayıcının veri koruması zafiyeti vücut bulursa veri koruma otoritesine bildirimde bulunmak zorundadır.

Bazı Avrupa Birliği ülkelerinde ise farklı uygulamalar söz konusudur. Örneğin, Almanya, belli bazı sektörlere ilişkin verilere ilişkin zafiyet gerçekleşmesi halinde pozitif bildirim yükümlülüğü getirmektedir. Banka ve kredi kartı verisi, idari bir soruşturmaya ilişkin veri, ticari sır vs. bu kapsamda pozitif bildirim yükümlülüğü getiren veri türlerindendir.

V. Eleştiriler

Amerika Birleşik Devletleri ve Avrupa Birliği ile Türkiye, siber güvenlik uygulamaları ve mevzuatları açısından karşılaştırıldığında Türkiye'nin, gerek uygulamaları gerekse mevcut mevzuatı bakımında bilişim teknolojisine ilişkin gelişmeleri belirgin bir şekilde geriden takip ettiği açıktır.

Türkiye'deki siber güvenliğe ilişkin mevzuat bünyesindeki düzenlemelerin genel nitelikte olması, cezai yaptırıma konu eylemlerin yoruma açık bırakılması uygulamada tutarsızlığa ve boşluklara neden olmaktadır. Öte yandan, söz konusu düzenlemelerin ve bu düzenlemelerin temeli olan siber güvenlik politikasının yalnızca siber güvenlik riskin gerçekleşmesi haline yönelik olması ve önleyici nitelikte tedbirleri içermemesi da Amerika Birleşik Devletleri ve Avrupa Birliği siber güvenlik politikaları ile karşılaştırıldığında ciddi noksanlıklar barındırmaktadır. Zira Türkiye'de veri korunmasına ve dolayısıyla siber güvenliğin sağlanmasına yönelik olarak, "risk gerçekleşmeden müdahale etmek" yönünde bir refleks bulunmamaktadır.

Bu kapsamda, evvelce değindiğimiz "pozitif bildirim yükümlülüğü" meselesine Türkiye'deki düzenlemeler ve uygulamak çerçevesinden bir kez daha bakmak gerekir. "Pozitif bildirim yükümlülüğü" esasen temelini Anayasa'dan almaktadır.

[7] Hekim, Hakan, *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları.*

[8] Önok, Murat, *Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği.*

Anayasa'nın 20. maddesi uyarınca, herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve "amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi" de kapsar. Dolayısıyla, bir kişiye ait verinin o veriye sahip olmaya, veriyi bilmeye, elinde tutmaya yetkili kimselerden başka üçüncü kişiler tarafından ele geçirilmesi, değiştirilmesi, bozulması vs. nihayetinde eyleme konu verinin amacı doğrultusunda kullanılıp kullanılamadığı takip edilemez bir noktaya ulaşmaktadır ve verinin ait bulunduğu kişinin bu hususta bilgilendirilmesi veriyi elinde bulundurana Anayasa tarafından yüklenmiş bir yükümlülüktür. Ancak, Türkiye'de bu yükümlülüğe tam anlamıyla bir uygulama alanı yaratan bir mekanizma hâlihazırda mevcut değildir; sektörel bazda düzenlemeler mevcuttur.

Örneğin; elektronik haberleşme sektörüne ilişkin olarak, bu sektörde faaliyet gösteren kurum/kuruluş ve kişilerin bünyesinde barındırdığı kendisine yahut başkalarına ait verilere yönelik bir siber güvenlik ihlalinin vücut bulması halinde, Bilgi Teknolojileri ve İletişim Kurumu'na bildirim yükümlülüğü söz konusudur. Ancak, bünyesinde farklı mahiyette olmak üzere aynı miktarda veri bulunduran başka sektör oyuncuları bu yükümlülüğe tabi değildir. Verinin mahiyetine göre koruma mekanizması kurulması anlaşılabilir bir politika olabilir. Bununla birlikte, ihlal halinde işleyecek herhangi bir telafi mekanizması bulunmamasının açıklaması yoktur.

Türkiye'de bu hususa çözüm getiren "Kişisel Verilerin Korunması Kanunu" hala taslak halindedir. Böylesine önemli bir meselenin hala ülke gündeminde önceliklendirilmemiş olması siber güvenlik açısından Türkiye'nin özen ve hassasiyet eksikliğine işaret etmektedir. Zira Amerika Birleşik Devletleri ve Avrupa Birliği üye ülkelerinde yerleşik bir uygulamanın mevcudiyeti, Türkiye'ye "siber güvenliğe ne kadar önem veriyoruz?", "siber güvenlik politikamız gerçekten de çağı yakalıyor mu?" gibi soruları tekrar sorması için bir başka nedendir.

VI. Türkiye'nin Siber Güvenlik Boşlukları İçin Atılması Gereken Adımlar

Siber güvenliğin hedefleri verinin erişilebilirliğinin, bütünlüğünün ve gizliliğinin sağlanmasıdır. Bu kapsamda, kamu kurumlarına, özel sektöre, üniversitelere ve bireylere önemli görevler düşmektedir. Siber güvenliğin korunmasının bireysel boyutunun yanında toplumsal bir boyutunun olduğu algısının Türkiye'de birey ve devlet politikası bazında yerleşmesi gerekmektedir. Bu doğrultuda, siber güvenlik kültürünün oluşturulması, veri tabanlarının korunması, kamu-özel işbirliğinin sağlanması, uluslararası işbirliği sağlanması ve en önemlisi siber güvenliğin sağlanmasına yönelik mevzuatın geliştirilmesi gerekmektedir.

Kurumsal olarak alınacak ufak tedbirler, ulusal siber güvenliğe önemli katkılar yapabilecek niteliktedir. İş birliği bunlardan en büyük öneme sahip unsurlardan biridir. Özellikle siber güvenlikten sorumlu kurumlar arasında hızlı bilgi paylaşımı sağlanması ve işbirlikleri bu kurumların etkinliğine olumlu etki edecektir. Sadece kamu kurumları arasındaki bilgi paylaşımı ve işbirliği değil, kamu ve özel sektör arasında da bilgi paylaşımı ve işbirliği mekanizmalarının kurulması oldukça önemlidir.[9]

Veri koruma politikasının siber güvenliğin sağlanması aşamasında temel yapı taşlarından biri olduğu unutulmamalı bu

[9] Hekim, Hakan, *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları.*

hususta gereken önceliklendirme yapılmalıdır. Taslak halindeki düzenlemelerin yürürlüğe girmesi ve ivedilikle uygulanması yönünde gerekli adımlar gecikmeden atılmalıdır. Gerçek bir siber saldırı ile karşılaşmadan evvel gerekli tedbir mekanizmaları kurulmalı ve işler hale getirilmelidir. Riskin gerçekleşmesini beklemek yerine bu riskin gerçekleşmesini önlemek siber güvenlik politikasının odak noktası olmalıdır.

Öte yandan, veri korunması ihlallerinin toplumsal boyutunun yanı sıra bireysel bir boyutunun olduğu ve bu hususun anayasal dayanakları olduğu noktası iyice irdelenmelidir. Zira anayasal bir hakkın kullanılmasını imkânsız kılan bir mekanizmanın sürdürülmesi kabul edilemez bir demodeliktir.

2015-2016 yıllarına ilişkin Siber Güvenlik Kurulu Eylem Planı kapsamında sürdürülen çalışmalar da, mevcut durum ve içinde bulunduğumuz zaman dilimi de göz önüne alınarak, bir an önce uygulamada yerini almalı ve mevcut mekanizmaların aksamasının önüne geçilmelidir.