EDAM Siber Politika Kağıtları Serisi 2

Türkiye'de Veri Gizliliği ve Gözetimi:

Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi

Doç Dr. H. Akın Ünver

Öğretim Üyesi, Uluslararası İlişkiler Bölümü,

Kadir Has Üniversitesi

Grace Kim

EDAM Araştırma Görevlisi

19 Şubat 2016

GİRİŞ

Aşırı bağlantılılığın (*hyper-connectivity*) norm halini aldığı günümüzde insanlar, araçlar ve ağlar daha hızlı, daha ucuz ve daha elverişli bir biçimde birbirlerine bağlıdırlar. Taşınabilir bilgisayarlardan akıllı telefon saatlerine uzanan 21. yüzyıl teknolojisi, bir hayli dijitalleştirilmiş dünyamızda kontrolsüzce toplanan ve analiz edilen büyük-çaplı verileri sermayeleştirmek üzerine kurgulanmıştır. Dijital teknolojinin günlük hayatımızın pek çok alanına entegre edilmesi bir yandan iletişim, eğitim ve serbest zaman etkinliklerini milyarlarca insana erişilebilir kılarken diğer yandan ise, kişisel gizliliği, devlet gözetimi ve siber korsanlığa tabi tutarak, gittikçe savunmasız hale getirmektedir.

Bireysel gizlilik haklarına saygı göstermek ve milli güvenliği korumak arasındaki hassas denge, veri gizliliğini toplumsal tartışmaların merkezine taşımaktadır. Gizlilik/güvenlik tartışmasının hem siyasal hem de ekonomik boyutları mevcuttur. Tartışmanın siyasi boyutu, milli istihbarat kuruluşlarının, terrörist tehditlerine karşı önlem almak ve diğer olası toplumsal hadiselerin önüne geçmek için vatandaşların ve yabancıların kişisel bilgilerini toplarlarken ne kadar esneme payına sahip oldukları ile ilgilidir. Tehdit unsurlarına karşı şahsi bilgisayar ve telefonları sürekli olarak denetleyen devlet-destekli gözetim programları, milyonlarca veriyi depolayan teknoloji şirketlerinin rızası olarak ya da olmaksınız, üstü kapalı bir biçimde faaliyet göstermekte, yasal gözetim faaliyetleri ve kişisel gizlilik haklarının yaygın ve kapsamlı ihlalı arasındaki ince çizgiyi çoğunlukla bulandırmaktadır. Pek çok ülke vatandaşlarına, özel hayatın gizliliğine dair anayasal ve yasal garantiler sunmaktadır. Gizlilik ve güvenlik arasındaki gerilim, gizlilik ihlalinin, kamuya daha fazla güvenlik sağlamak için gerekçelendirilmesi ve hükümetlerin gözetim programlarını hukuki olarak nasıl yürüttüğü noktalarında su yüzüne çıkmaktadır.

Aynı şekilde bu tartışmanın ekonomik boyutu da kapsamlı bir değerlendirmeyi gerektirmektedir. Bireylere ait şahsi bilgilerin her gün meydana gelen sayısız uluslararası işlem boyunca korunduğu garantisini veren veri gizliliği, modern ekonomiler için temel bir ilkedir. Çevrimiçi alışverişten, başka ülkerlerde yaşayanlarla mesajlaşmaya; bulut bilişimden veri madenciliğine uzanan günümüzün dijital olarak bağlı dünyası, uluslararası serbest piyasaları idame ettirmek için gerekli olan gizliliğin korunması konusunu yeni tehditlerle karşı karşıya bırakmaktadır. 2000'den beri Avrupa Birliği (AB) ve Amerika Birleşik Devletleri (ABD) arasındaki ticari işlemlerde veri gizliliğinin korunması yönelik Güvenli Liman Anlaşması'nın (Safe Harbor) Avrupa Adalet Divanı – ATAD tarafından kısa süre önce

feshedilmesi, 2016 yılı başında Güvenlik Kalkanı adini taşıyan yeni bir metnin müzakere edilmesini zorunlu kılmıştır.

Haziran 2013 tarihinde ABD Ulusal Güvenlik Teşkilatı'nda yüklenici olarak görev yapan Edward Snowden'ın gizli belgeleri tüm dünyaya sızdırması, gizlilik/güvenlik tartışmasını yepyeni bir boyuta taşımıştır. O zamandan beri hükümetler, tasdik edilmiş iç gözetim programlarına karşı yükselen toplumsal itirazı yatıştırmakla uğraşmaktadır. Paris ve San Bernardino gibi şehirlerde ortaya çıkan terörist saldırılarının göstermiş olduğu gibi, kişisel özgürlüklerin korunması ve kamu güvenliğinin sağlanması arasındaki hassas dengenin muhafaza edilmesi hükümetlerle vatandaşlar arasında yeni bir analyış üzerinde mutabık kalınmasını gerekli kılmaktadır. Şikayet paylaşımı, iletişim ve mobilizasyon için sık sık alternatif kamu sahası rolü üstlenen İnternet ve dijital teknolojinin yaygınlaşması, görüş ayrılıkları ve siyasi muhalefet için gerekli olan geleneksel kamu kanallarından mahrum olan ülkeler için ciddi bir tehdit teşkil etmektedir.

Wall Street'i İşgal Et (Occupy Wall Street) ve Arap Baharı protestolarının dünya başkentlerini sarsmasıyla veri erişimi ve İnternet (sosyal medya kullanımı ve gizlilik) konuları 2011 senesinde anaakım tartışmalar arasında küresel boyutta yer almıştır. Twitter, Facebook, Youtube ve Instagram gibi bilgiye hızlı erişim ve yayılım sağlayan sosyal medya platformları, bu tartışmaların organizasyonel boyutlarına kolaylık sağlamış ve ulaştırmaya çalıştıkları mesajın içselleştirilmesine olanak tanımıştır. 2011 senesini şekillendiren bu yaygın gösteriler ve muhalif hareketler Türkiye'ye 2013 tarihinde İstanbul Gezi Park'ta başlayan Haziran olaylarına da yansımış, sosyal medya aracılığıyla diğer şehirlere sıçramıştır. İşte tam o günlerde İnternet, sosyal medya ve veri siyasası Türkiye'deki anaakım tartışma konuları olmuş, devlet-toplum ilişkisindeki yeni sınır kapılarını oluşturmuştur.

Dünya Bankası verilerine göre, Türkiye'deki İnternet penetrasyonu %51'e ulaşmıştır.[1] Bu da yaklaşık 80 milyon olan toplam nüfusun neredeyse yarısının, bilgisayar ya da cep telefonu gibi bir cihazla, İnternet bağlantısı gerçekleştirdiğini sergilemektedir. Ayrıca, genel ekonomik büyüme ve satın alma gücündeki artış beraberinde, İnternet ve sosyal medya kullanımı son on yıl içerisinde hızlı bir artış göstermiştir. 2003'te İnternet kullanıcılarının sayısı yalnızca 8,130,188 iken bu rakam 2014 senesinde 35,358,888'e ulaşmıştır[2]. Benzer şekilde, İnternet

[1] Dünya Bankası, 'Internet users (per 100 people)' Erişim tarihi: 31 Ocak 2016, http://data.worldbank.org/indicator/IT.NET.USER.P2

[2] Internet Live Stats. 'Turkey Internet Users'. Erişim tarihi: 2 Ocak 2016, http://www.internetlivestats.com/internet-users/turkey/

2003 senesinde nüfusun %12.3'üne ulaşırken, 2014'te bu %46.6 olmuştur[3]. Ancak, İnternet erişimindeki hızlı artışın Türkiye'ye özel olmadığının altı çizilmelidir. Türkiye'deki bu trend İnternet erişimindeki küresel artışa paralel seyretmektedir zira Türkiye'nin dünya çapındaki İnternet kullanıcı payı 2003-2014 boyunca ortalama %1.24 olarak kalmıştır[4]. Türkiye, küresel İnternet erişimi sıralamasında 15. sıradan (2003) 17. sıraya (2014) düşmüştür. Bu önemli ve aydınlatıcı bir bakış açısı sunmaktadır: her ne kadar, çevrimiçi ifade özgürlüğü veya sosyal medya sınırlamalarında karşılaşılan problemler Türkiye'ye has ve kültürüne-özgü meseleler olarak algılansa da bunlar, diğer ülkelerin sanal devlet-toplum ilişkileri çerçevesinde farklı seviyelerde karşılaştıkları küresel olaylardır. Dolayısıyla, Türkiye'nin veri özgürlüğü, kişisel veri veya çevrimiçi ifade özgürlüğü gibi konularla küresel alanda nasıl etkileşim gösterdiği önemle incelenmelidir.

ARKA PLAN

Teknolojik ilerlemeler İnternet'in yaratıcılarının hayallerinin çok daha ötesinde gelişmiştir. Dijital ve İnternet teknolojileri günlük hayatımızı baştan aşağı değiştirmekle kalmamış, politika, kamuoyu ve sivil katılımı da kökten yenilemiştir. İnternet ve onu kullanmak için yeni yollar keşfetmeye çabalayan teknoloji firmaları küreselleşmeyi hızlandırıp, birbirinden farklı ülkeleri bir araya getirirken, dünyanın dijitalleşmeye devam etmesi eski mevzuatları yeniden değerlendirmeyi ve onları yeni beliren zorluklara uygulanabilir hale getirmeyi şart koşmuştur. Örneğin, ABD Ulusal Güvenlik Teşkilatı'nın devlet gözetim proglamlarının detaylıca tüm dünyaya yayılması devletlerin, ulusal güvenlik altında vatandaşlarının özel hayatlarını ne ölçüde ihlal edebilecekleri tartışmasını yeniden alevlendirmiştir. Şifreleme (encryption) tartışması, özel şirketlerin servislerini kullanan müşterilere mi, işletmelerini düzenleyen devlet organlarına mı daha fazla sorumluluk taşıdıkları sorusunu gündeme getirmiş, devlet müesseseleri ve teknoloji devleri arasında uzlaşmayı engelleyen bir başka tartışmalı konu olarak gündemde yerini almıştır.

Gizlilik/güvenlik tartışması, bireysel vatandaşlar, sivil toplum kuruluşları, akademik çevre, işletmeler, merkezi hükümetler ve hükümetlerarası kuruluşları kapsayan çok çeşitli bir paydaş spektrumundan oluşmaktadır. Geçtiğimiz yıllarda İnternet Hizmet Sağlayıcıları (İHS) kamu tartışmalarının özellikle merkezinde yer almıştır. Bireysel teknoloji firmalarının yanısıra İHS, bir bireyin tek bir cihaz ya İnternet sayfasındaki çevrimiçi aktivilerine erişim sağlamakla

[3] A.g.e.
[4] A.g.e.

kalmayıp, aynı zamanda tek bir İnternet bağlantısı üzerinden gerçekleşen tüm cihaz, İnternet sayfası ya da uygumalardaki toplam çevrimiçi aktivitelerinin karışımına direk erişim sağlayabilmektedir. Bu şirketler, hedefe yönelik yapılan reklamcılığın, ve sosyal medya şirketlerini bu bağlamda geride bırakmanın ne denli kârlı olduğunun farkına varmaya başlamışlardır. Başka bir deyişle, İnternet üzerinde toplanan dijtal bilgi bolluğu çoğalmaya devam edecek, gerekli gizlilik tedbirlerini devreye sokmak mesuliyeti hükümetlere kalacaktır.

Kişisel Veri Korunması Kanunu tasarısı TBMM'de tartışılırken, Avrupa, Amerika Birleşik Devletleri, Çin, Rusya ve İran gibi devletlerin gizlilik mevzuatlarının incelenmesi, gizlilik ve güvenlik kaygılarını dengelemek için hangi liberal ve otoriter siyasa seçeneklerinin olduğunu görmek açısından önemlidir.

Tablo 1 - Kişisel Veri Korunması: Anahtar Terimler[5]

Veri	Veri - (a) belirli bir amaç uğruna sağlanan talimatlara otomatik olarak faaliyet gösteren araçlar vasıtasıyla işlenen, (b) söz konusu araçlar tarafından işlenmesi niyetiyle kaydedilen, (c) konu ile ilgili bir dosyalama sisteminin parçası olarak ya da konuyla ilgili bir dosyalama sisteminin parçasını oluşturması niyetiyle kaydedilen bilgidir.
Kişisel Veri	Kişisel veri - a) veri, (b) veri idarecisinin hükmü altında olan veya olma ihtimali yüksek olan, ve birey ile ilgili herhangi bir fikrin ifadesi ve veri idarecisinin veya bireyle ilgili olan herhangi bir kimsenin niyetine işaret eden, bireyle ilgisi olan veri ya da diğer bilgiler tarafından tanımlanan veri demektir.
	Hassas kişisel veri - (a) veri öznesinin ırksal ya da etnik kökenine, (b) siyasi görüşlerine, (c) dini ya da diğer inançlarına, (d) herhangi bir sendika üyeliğine, (e) fiziksel veya akli sağlık durumuna, (f) cinsel hayatına,

[5] Bilgi Komiserliği, Birleşik Krallık. 'Key definitions of the Data Protection Act'. Erişim tarihi: 2 Ocak 2016, https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Hassas Kişisel Veri	(g) herhangi bir suç unsurunun işlenmesi ya da işlendiğinin iddia edilmesine, (h) işlenen ya da işlendiği iddia edilen herhangi bir suç unsuruna dair yargılamaya ilişkin bilgileri içeren hassas bilgilerdir.
İşleme	Bilgi veya verinin işlenmesi şu anlama gelmektedir; veri veya bilginin elde edilmesi, kayıt edilmesi veya tutulması ya da bilgi veya veri üzerinde aşağıdakilerin de arasında bulunduğu işlemlerin birinin veya bir kaçının yapılması: (a) düzenleme, uyarlama ya da değiştirme, (b) geri alma, danışma ya da kullanım, (c) yayın, dağıtım veya başka bir yolla erişime açık hale getirerek açığa çıkarma veya (d) düzenleme, bir araya getirme, engelleme, silme veya imha.
Veri Öznesi	Veri öznesi kişisel verinin ilgilendirdiği şahıs anlamına gelmektedir.
Veri İdarecisi	Herhangi bir kişisel verinin ne amaçla ve ne yolla işlendiğine veya işleneceğine (tek başına, birlikte veya diğer insanlarla ortak olarak) karar veren kişidir.
Veri İşleyicisi	Kişisel veri hususunda veri işleyicisi, veri idarecisinin adına verileri işleyen (veri idarecisinin çalışanı haricinde kalan) kişi anlamına gelmektedir.
Üçüncü Parti	Kişisel veri hususunda üçüncü taraf – (a) veri öznesi, (b) veri idarecisi, veya (c) veri işleyicisi veya veri işleyicisi veya idarecisi adına veriyi işleme yetkisi olan kişiler haricinde kalan partidir.

ÖNEMLİ VAKA ÇALIŞMALARI

Avrupa

Birçok ülke teknolojik değişimlerin hızlı temposuna ayak uydurmakta zorlanırken, Avrupa mevzuatı veri gizliliği ve veri koruması haklarını 10 yıldan uzun süredir açıkça sağlamaktadır. 2000 senesinde beyan edilen ve tüm AB üyesi ülkeler için bağlayıcı olan Avrupa Birliği Temel Haklar Bildirgesi özel olarak gizlilik, veri koruması ve haksızlığa uğranması halinde etkin yasal çözümler sağlanması haklarını özel olarak korumaktadır. Lizbon Antlaşması'nın 2009 senesinde yürürlüğe girmesiyle birlikte veri koruması temel bir hak haline gelmiş ve Avrupa'nın devletlerin gizlilik koruma mekanizmalarını gevşeterek daha yayılmacı güvenlik önlemleri benimsemeye meyletmesine karşı koyan gizlilik kanunlarını daha da sağlamlaştırmıştır.

Avrupa İnsan Hakları Sözleşmesi (AİHS) kişisel veriyi, "kimliği saptanan veya saptanabilen özel kişi[ye]" ait olarak; özel kişiyi ise "özellikle kimlik numarası veya fiziksel, fizyolojik, akli, ekonomik, kültürel veya sosyal kimliğine dair bir veya birden fazla etken vasıtasıyla doğrudan veya dolaylı olarak tanımlanabilecek kişi"[6] olarak tanımlamıştır. Avrupa İnsan Hakları Mahkemesi tarafından infaz edilen AİHS'nin 8. Maddesi kişisel verilerin, verinin öznesinin rızası olduğu ya da işlenen verinin önceden onay verilen eylemlerin gerçekleştirilmesi için gerekli olduğu ve gerekli koruyucu tedbirlerin alındığı haller haricinde işlenmesini yasaklamaktadır.

Avrupa'da, Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (AK) kişisel gizliliği ve veriyi korumak için yasal tedbirlerin uygulanmasından sorumlu diğer iki ana kurumdur. OECD'nin Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri (1980) de bireylerin gizlilik haklarını teminat altına almaktadır, ancak gözetlemeye karşı koruma sağlamaktan çok verinin uluslararası veri transferleri için toplanması, işlenmesi ve dağıtılmasıyla alakalıdır. Bunun ardından 1981'de AK'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Avrupa gizlilik haklarının yeni teknolojiye uyarlanmasının ilk denemesi olarak gizlilik haklarını daha da ileriye götürmüştür. Sözleşmenin özetinde belirtildiği üzere, "Bu sözleşme bireyi kişisel verilerin toplanması ve işlenmesinin suiistimal edilmesine karşı koruyan ilk bağlayıcı uluslararası belgedir … Kişisel verilerin toplanması ve işlenmesine dair teminatlar sağlamanın yanı sıra, kişinin ırkı, siyasi görüşleri, sağlığı, dini, cinsel yaşamı, sabıka kaydı

[6] Avrupa Birliği, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

vb. gibi "hassas" bilgilerin münasip yasal tedbirlerin olmaması durumunda işlenmesini yasaklamaktadır."[7]

Gizlilik konusundaki bu teminatlara rağmen Kişisel Veriler Sözleşmesi, devletlerin ulusal güvenlik gerekçesiyle vatandaşlarının gizliliğini ihlal etmesine olanak sağlayan bir şerh içermektedir. Anlaşmanın 9. Maddesi'ne göre istisnalara, "devlet güvenliği, kamu güvenliği, devletin mali çıkarları söz konusu olduğunda veya yasadışı faaliyetlerin bastırılması amacıyla"[8] olduğunda izin verilecektir. Teknolojinin birçok alanına uygulanabilir olsalar da, ne OECD ilkeleri ne de AK Kişisel Veri Sözleşmesi günümüzde gizlilik ve güvenliğin hassas dengesinin karşı karşıya olduğu güçlükleri yeterli düzeyde düzenlemektedir. Ancak 1995 senesinde uygulanan AB Veri Koruma Direktifi ve 2012'de teklif edilen Veri Koruma Yasası Avrupa dijital gizlilik koruma yasalarının köşe taşlarını uzun yıllarca oluşturmuştur.

15 Aralık 2015 tarihinde Avrupa Komisyonu, Avrupa Parlamentosu ve Avrupa Konseyi Genel Veri Koruma Reformu üzerine uzlaşmıştır; reform, farklı ülkeler ve sektörlerde var olan dağınık mevzuatı bir araya getirerek, resmi olarak kabul edilmesi halinde Avrupa veri koruma yasaları için tek bir yasal çerçeve oluşturacaktır.[9] Genel Veri Koruma Mevzuatı ve Veri Koruma Direktifi reformun iki ana aracıdır. Veri Koruma Reformu, Avrupalılara kendi kişisel verileri üzerinde daha fazla kontrol vermekte, aynı zamanda polislere ve yargı sistemine devam eden davalarda verileri daha verimli incelemek için araçlar sağlarken, bir yandan da kolluk kuvvetleri yetkililerine davalarda kurbanların, tanıkların ve şüphelilerin verilerini koruma zorunluluğu getirmektedir.

Reform paketinin "tek uğrak noktası" olması amaçlanmış, resmi olarak kabul ediliş tarihinden sonra iki seneliğine geçerli olması planlanmıştır.[10] Dahası firmalar artık, verileri hacklendiği zaman bireyleri bilgilendirmekle yükümlü ve belirlenen koşullar sağlandığında Avrupa vatandaşlarına "unutulma hakkı" sağlamak zorundadırlar.[11] Genel Veri Koruma Reformu aynı zamanda küçük ve orta büyüklükteki işletmeler (KOBİ) bağlamında da veri gizliliğine

---

[7] Avrupa Konseyi, "Details of Treaty No.108" http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[8] Avrupa Konseyi, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (European Convention Series – No.108), 1 Ekim 1985, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

[9] Avrupa Komisyonu, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 Aralık 2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm

[10] Avrupa Komisyonu, "Reform of EU data protection rules," Son güncelleme 9 Şubat 2016, http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[11] Avrupa Komisyonu, "Questions and Answers: Data protection reform," 21 Aralık 2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

değinmektedir. Reform, AB'nin 28 üye ülkesinin hepsinde geçerli olacağından düzene koyulmuş ve kolay erişilebilen veri gizliliği kanunlarının sınır ötesi ticareti ve ekonomik kalkınmayı geliştirmesi hedeflenmiştir. AB Adalet, Tüketici Hakları ve Cinsiyet Eşitliği Komiseri Vera Jourova'nın belirttiği üzere, "Vatandaşlar ve işletmeler, dijital çağa uygun, hem sağlam koruma sağlayan, hem de Avrupa Dijital Tek Pazarı'nda fırsatlar yaratacak ve inovasyonu teşvik edecek açık kurallardan kar sağlayacaktır. Ve polis ve yargı mercileri için uyumlulaştırılmış veri koruma kuralları, Üye Devletler arasında kolluk kuvvetlerinin karşılıklı güvene işbirliğini kolaylaştıracak, böylelikle Avrupa Güvenlik Ajandası'na katkıda bulunacaktır."[12]

Avrupa genellikle politikalarında güvenlik odaklı olmaktansa gizlilik odaklı olmakla tanımlansa da, Orta Doğu'dan dönen cihatçıların yarattığı terörist tehdidi, liberal Batı demokrasilerinin gizlilik yasalarını yeniden gözden geçirerek daha fazla gözetlemeye izin vermesine yol açmıştır. Wall Street Journal'ın devletlerin teknoloji firmalarından talep ettiği kullanıcı bilgileri üzerine yaptığı analize göre, "Avrupa Birliği'ndeki devletler ve kolluk kuvvetleri kurumları, Microsoft, Google, Apple, Facebook ve Twitter'dan 2015'in ilk yarısında yaklaşık 63000 kullanıcı bilgisi talebinde bulunmuştur, bu da bir önceki seneye kıyasla %24'lük bir artışa tekabül etmektedir."[13] AB'nin Birleşik Devletler gibi diğer liberal Batı demokrasilerine nazaran daha büyük bir gizlilik savunucusu olduğuna dair genelgeçer bir kanı olsa da, bu tarz kıyaslamalar devletlerin, ulusal güvenlik adı altında almaya gönüllü oldukları, artan güvenlik önlemlerini ortaya koymaktadır.

Amerika Birleşik Devletleri

Terörizme karşı açılan savaş, tartışmaları dünya çapında yenilemiştir; Yalnızca Avrupa'da değil, ABD'de de devletlerin vatandaşlarının güvenliğini sağlamak için kişisel özgürlüğü ne derecede ihlal edecekleri konusu gündemdedir. World Wide Web muciti ve koruyucusu olan ABD, İnternet'in yönetimi ve düzenlemesi veya eksikliği ile ilgili oldukça etkin bir role sahiptir. Benzer biçimde ABD genellikle gizliliği güvenliğe önceliklendirmektedir. Ancak, 11 Eylül 2001 terrör saldırınsan itibaren, gerek iç gerekse dış politikasında daha güvenlik-odaklı bir yaklaşım benimsediği görülmektedir.

---

[12] Avrupa Komisyonu, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 Aralık 2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm

[13] Sam Schechner, "Tech Companies bring Battle over Data to Davos", *Wall Street Journal* http://www.wsj.com/articles/u-s-tech-companies-bring-encryption-battle-to-davos-1453320950?mod=djem10point&cb=logged0.5909027620218694

Ulusal Güvenlik Teşkilatı'nda yüklenici olarak görev yapan Edward Snowden'ın ABD'nin yaygın iç gözetim programlarını açıkca gözler önüne seren gizli belgeleri sızdırması, Washington'i yurtiçindeki ve yurtdışındaki taraftar ve karşıtların bitmek bilmeyen eleştirisi altında bırakmıştır. Bu durum, terörizm karşıtı mevzuatın desteklediği gözetim programlarının yalnızca yasal boyutunu değil aynı zamanda niyetlerinin sorgulanmasını doğurmuştur. ABD Anayasası'nın 4. Maddesinde yer alan sebepsiz arama ve tutuklamaya karşı koruma hususu, vatandaşları hukuka aykırı gözetim programlarından korumak için düzenlenen her türlü gizlilik mevzuatının temelini oluşturmaktadır. ABD Adalet Bakanlığı'nın Kişisel Mahremiyet Yasası (1974), devlet kurumlarının kayıt sistemlerinde yer alan bireylere ilişkin bilgilerin toplanması, muhafazası, kullanımı ve yayılması için adeletli bir bilgi uygulama kılavuzu geliştirmiştir[14]. Amerikan vatandaşlarını daha iyi koruyabilmek adına Elektronik İletişim Güvenlik Yasası (1986), kolluk kuvvetlerinin kişisel iletişime olan erişimini kısıtlamış, hukuka aykırı olarak elde edinilen bilginin ifşa edilmesini cezai yaptırıma tabi bırakmıştır.

Belki de şu ana kadar karşılaşılan ve devlete daha fazla gözetim yetkisi tanıyan mevzuatlar arasında yer alan en tartışmalı ve yüksek profilli olanı, daha çok Vatanseverlik Yasası olarak bilinen, Terörizmi Durdurmak ve Engellemek için Gerekli Doğru Araçların Sağlanması Yasası'dır (2001). Bu yasa, ABD'nin gözetim gücünü genişletmiş, kolluk kuvvetlerine, elektronik gözetim yapmaları ve telefonları dinlemeleri için daha fazla imkan ve faaliyet alanı tanımıştır[15].

Ulusal Güvenlik Teşkilatı olayının açığa çıkması, devlet destekli toplum gözetim programlarına karşı dünya çapında bir protestoyu da beraberinde getirmiş, ABD ve teknoloji firmaları arasında süregelen gerginliği daha da kötüye götürmüştür. İlişkileri düzetlmek amacıyla, Cumhurbaşkanı Obama ve Savunma Bakanı Ashton Carter gibi üst düzey devlet çalışanları, teknoloji yöneticileriyle birlikte Beyaz Saray'ın dijital ajendasını tartışmak ve daha iyi bir işbirliği için gerekli olan potansiyel siyasa alanları geliştirmek için Silikon Vadisi'ne gitmişlerdir. Ayrıca, devlet gözetim programlarını limitlemek ve Vatanseverlik Yasası'nın tartışılan bazı boyutlarını durdurmak için ABD Kongresi Özgürlük Yasası'nı (2015) çıkarmıştır. Vatanseverlik Yasası'nın süresinin dolmasından bir gün önce Özgürlük Yasası, Amerikan vatandaşlarının telefon kayıtlarının yığın halinde toplanmasına son vermiş,

[14] Amerika Birleşik Devletleri Adalet Bakanlığı "Privacy Act of 1974" Erişim tarihi: 24 Ocak 2016, http://www.justice.gov/opcl/privacy-act-1974

[15] Amerika Birleşik Devletleri Adalet Bakanlığı, "The USA PATRIOT Act: Preserving Life and Liberty" Erişim tarihi: 28 Ocak 2016, http://www.justice.gov/archive/ll/highlights.htm

ancak Vatanseverlik Yasası'nın olanak sağladığı çoğu gözetim hükmünün hala yürürlükte olduğunu savunan gizlilik yandaşlarını tam anlamıyla tatmin edememiştir.[16] Özgürlük Yasası özel şirketlerin veri saklama güçlerini ellerinden aldıktan ve kamu yararına Dış İstihbarat Gözetim Mahkemesi müzakerelerini destekledikten sonra, bazı ABD Kongre üyeleri devletin güvenlik güçlerini fazlasıyla kaybettiğini öne sürmüş, bunun başka bir terörist saldırısı olasılığını güçlendirebileceğini savunmuştur.[17]

Çin

Birçok otoriter rejimde olduğu gibi Çin de, yerel İnternet'ini sıkı olarak kontrol etmekte ve vatandaşlarının gizlilik hakları yerine ulusal güvenliği korumayı (bu kavram ne kadar geniş tutulursa tutulsun) tercih etmektedir. Sayıları 1 milyarın üstünde olan Çin vatandaşları Pekin'in ülkeye hangi bilgilerin, malların ve hizmetlerin girip çıkacağı üzerindeki sarsılmaz kontrolüne uzun süredir alışkın olsalar da, dijital teknolojinin kullanım alanlarının ve erişiminin yaygınlaşması, devlet üzerinde kamunun dünyanın geri kalanıyla bağlanma arzusunu kısıtlamak için daha çok baskı yaratmıştır.

Çin içeride ve dışarıda aldığı önlemleri meşrulaştırmak için İnternet altyapısını Devlet Başkanı Xi Jinping tarafından ortaya atılan "siber egemenlik" ilkesine dayandırmıştır. Siber egemenlik kavramı katı siyasi ve ekonomik kontrollerin siber dünyaya da uzanmasını içermekte ve Pekin'in "yerli İnternet'ini geliştirme, düzenleme ve idare etmesini" ve "İnternet'ini yabancı saldırılara ve sızmalara karşı savunmasını"[18] sağlamaktadır. Diğer bir deyişle Çin hükümetinin siyaset, ekonomi ve toplum üzerindeki sıkı kontrolü dijital dünyaya da uzanmaktadır.

Vatandaşlarının İnternetteki faaliyetlerini katı bir biçimde takip etme ve düzenlemenin yanı sıra Çin aynı zamanda, ithal ve ihraç ettiği teknolojik ürünler üzerinde sıkı bir kontrol sağlamakta, sıklıkla yerli üreticilerinin ve pazarlarının gelişmesini sağlamak için ulusal güvenlik kisvesi altında yabancı menşeli ürünleri ve hizmetleri yasaklamaktadır. Pekin ülkenin batı ucunda kalan Sincan bölgesindeki etnik Uygurlardan kaynaklanan radikal

---

[16] Sabrina Siddiqui, "Congress passes NSA surveillance reform in vindication for Snowden," *The Guardian*, 3 Haziran 2015, http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden.

[17] Alan Yuhas, "NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened," *The New York Times*, 2 Haziran 2015, http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden.

[18] Scott Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance" Chinafile, 19 Şubat 2015, https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance

İslamcılık tehdidini devletin gözetleme güçlerini arttıracak güvenlik kanunları geçirmesinin temel sebeplerinden biri olarak göstermektedir.

Rusya

Her ne kadar Rusya Federasyou demokratik idealleri ve kurumları benimsediğini ileri sürse de, Vladimir Putin başkanlığındaki ülkenin giderek daha otoriter olan ölçüleri yürürlüğe koyduğu görülmektedir. Sovyet Rusya Devleti Güvenlik Komitesi'nin (KGB) modern halefi olarak faaliyet gösteren Federal Güvenlik Servisi (FGS), Operasyonel-Araştırmacı Ölçü Sistemleri programı ile yurtiçindeki İnternet trafiği ve iletişimini yakından gözlemlemektedir. 1980'lerde başlayan bu program, yerel FGS bürolarını İnternet Hizmet Sağlayıcı'ları (İHS) ve telekommünikasyon trafiğine binlerce millik yeraltı kabloları aracılığıyla bağlayarak, ağ işletmecilerini ve İHS'larını, verilerini devlete erişebilir kılmaya zorunlu tutmuş böylelikle Rusya'daki bütün elektronik iletişimin önünü yasal düzeyde kesmiştir.

Kamuda telekomünikasyon hizmetleri, iletişim teknolojisini ve kitle iletişimi gözetlemekten sorumlu olan Rusya federal hizmeti, Roskomnadzor'dur. Her ne kadar Rusya, yasama ve yargı süreçlerinde demoktratik idealleri desteklediğini savunsa da, Putin rejiminin otoriter yaklaşımı siber alanı da kapsamaktadır. Rusya son bir kaç sene içerisinde, uluslarası forumlarda fiziksel sınırlara tabi olan ulusal İnternet yönetişimi oluşturulması çağrısında bulunmuş, Rus vatandaşlarına ait verileri saklayan Amerikan şirketlerini, Rus topraklarında depolama merkezleri açmaya zorunlu kılmıştır[19].

İran

İran'da gözetim, sansür ile bir arada yürütülmektedir, çünkü muhafazakar hükümet bu ikisini, rejimi tehdit edecek unsurlara karşı savunmak, ulusal güvenliği korumak ve vatandaşları ve bilgiyi kontrol altında tutmak için kullanmaktadır. Facebook, Twitter, Instagram ve Youtube gibi popüler uluslarası sosyal ağ oluşturma siteleri yasaklanmış olmalarına rağmen İran hükümeti bu siteleri, herhangi bir şüpheli aktivite olasılığı için gözetim altında tutmaya devam etmektedir. Hükümetin çelişkili gözetim politiklarına en güzel örnek, aslında İran halkının

[19] Julien Nocetti, "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy" Internet Policy Review Cilt 4 Sayı 4, 10 Kasım 2015, http://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy

tamamı için yasaklanmış olan Ayatollah Ali Khamenei hesabının, pek çok farklı sosyal medya mecrasında yer almasıdır.

2009'ta gerçekleşen Yeşil Hareket protestolarının akabinde İran, vatandaşlarını takip etmek için sağlam bir gözetim sistemini yürürlüğe koymuştur. Her ne kadar bu politikalar Yeşil Hareket'ten önce gelseler de, 2009'da Mahmoud Ahmadinejad'in başkanlık seçim zaferine karşı çıkmak için düzenlenen kitlesel siyasi protestolar hükümeti, halihazırda mevcut olan İnternet filtre araçlarını, elektronik gözetim ve bilgi manipülasyonunu destekleyen bir mevzut aracılığıyla sıkılaştırmaya sevk etmiştir[20]. İran'da yaşayan pek çok gencin bu harekette yer alması hükümeti, karşıt görüşlü olan sahışların sosyal medya hesaplarını incelemeye, yazdıklarına ve okuduklarına daha fazla anlam yüklemeye itmiştir[21].

İran'daki İnternet siyasasına göz kulak olan en üst mercii, 2012 senesinde Dini Lider Ali Khamenei'nin emri üzerine kurulan, Siber Uzay Üst Kurulu'dur[22]. Çevrimiçi içeriğe olan erişimi kontrol eden kuruluş Suçlu İçerik Olaylarını Tespit eden Çalışma Grubu'dur. 2009'da kurulan bu çalışma grubunun üyeleri Khamenei'nin yetkilendirmesiyle, kamu namusuna ve ahlakına, kutsal İslamik değerlere, güvenlik ve kamu barışına ve kamu kurumları ve kuruluşlarına aykırı bildirim gönderenleri tespit etmekle yükümlüdür[23].

Belki de İran'ın gözetim programları arasında en çok bilineni Ankaboot (bir diğer adıyla, Örümcek) Projesi'dir. Her ne kadar projenin başlangıç tarihi 2014 olsa da proje kamu tarafından ilk defa 31 Ocak 2015 senesinde kabul edilmiştir. Programın amacı, yolsuzluğu yayan ve Avrupai yaşam tarzını destekleyen Facebook sayfalarını ve aktivilerini yok etmektir[24]. İran Devrim Muhafızları Siber Savunma Komutanlığı'na bağlı olan Organize Siber Suç Merkezi, Örümcek'in operasyonlarını kontrol etmekte, ülkenin siber gözetim birimi olarak faaliyet göstermektedir. Ocak 2015'in sonlarına doğru, 130 Facebook sayfası kapanmış, 12 vatandaş tutuklanmış ve 24 vatandaş gözaltına alınmıştır[25]. İran Amerikan teknoloji firmalarını rejiminin istikrarına karşı tehdit olarak görse de, Amerikan firmalarının

[20] Irene Poetranto, "Since the Green Movement: Internet Controls in Iran, 2009-2012" Open Net Initiative, 15 Şubat 2013, https://opennet.net/blog/2013/02/after-green-movement-internet-controls-iran-2009-2012
[21] Martin C. Libicki, "Iran: A Rising Cyberpower?" The RAND Blog, 16 Aralık 2015, http://www.rand.org/blog/2015/12/iran-a-rising-cyber-power.html
[22] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," Kasım 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf
[23] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," Kasım 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf
[24] Arta Shams, "The State of Surveillance in Iran's Cyberspace" Azad Tribune, 14 Mayıs 2015, https://www.article19.org/azad-resources.php/resource/37964/en/the-state-of-surveillance-in-iran%E2%80%99s-cyberspace
[25] A.g.e.

İran rejiminin gözetleme ve bloklama teknolojisini asıl temin edenler oldukları söylenebilir. ABD bu tarzda teknolojileri satmaya yönelik sözleşmeleri yasaklamış olsa da, bu tip firmaları tespit etmekte zorlanmaktadır[26].

İran siber kolluk kuvvetleri İnternet'i, herhangi bir siyasi muhalafet ya da Şeriat Kanunu'nun ihlalı çercevesinde kontrol etmektedirler. Her ne kadar ülkenin gözetim programlarına ait pek çok detay tasdik edilemese de, İran Siber Polis Şef'i (FATA) gibi devlet adamları, Viber ve Whatsapp gibi mesajlaşma uygulamalarının kullanıcılarını yakından takip ettiklerine dair bir kamu açıklamasında bulunmuşlardır[27]. Ayrıca Tahran, ülkede faaliyet göstermeye devam etmek için ulusal kriterlere ayak uydurmak zorunda kalan Telegram gibi yüksek şifreli mesajlaşma uygulamalarına bile baskı uygulamayı başarmıştır[28].

Tahran İnternet'te bulunan içeriği ve erişimi kontrol altında tutmak için geliştirdiği ölçülerin sıkılığını gitgide arttırmıştır. Ulusal Bilgi Ağı'nın (UBA) kurulmasıyla İran, İnternet'in balkanlaştırılması anlamında kesin adımlar atan ülkeler listesine katılmıştır. Her ne kadar UBA'nın 2016 başlarında yürürlüğe konması planlansa da, programın karşılaştığı gecikmeler nihai başlangıç tarihini belirsiz kılmaktadır. UBA yürürlüğe girdiğinde halihazırda var olan sınırlamalar daha da katılaşacaktır. İran Uluslarası İnsan Hakları Kampanyası'nın hazırlamış olduğu bir rapora göre, İran'daki bütün İnternet erişimi yalnızca devletin erişebildiği kanallar aracılığıyla gerçekleşecek, devlet kurumları İran içerisinde ve ulusal Internet kapsamındaki bütün iletişime erişim sağlayacak, yetkililer diledikleri gibi küresel Internet erişimini engelleyebilecek ve böylelikle, İran'ın yurtiçindeki ağlarına yurtdışındaki kullanıcılar tarafından erişimi kısıtlayıp, engelleyebileceklerdir[29]. Kişisel güvenlik haklarını savunan uygun bir mevzuatın olmaması taktirde UBA'nın tamamlanması, İran'daki bütün vatandaşların çevrimiçi aktivitelerini ülkenin güvenlik ve yasama kurumlarıyla paylaşacakları anlamına gelmektedir.

Bilgi ve teknolojinin bütün dünyada olduğu gibi İran'da da yayılması, muhafazakar İranlıların vatandaşların çevrimiçi hareketlerini ve dijital içeriği kontrol edecek devlet mekanizmaları geliştireceğine işaret etmektedir. 2012 senesinde İran İnternet kafe sahiplerinin kullanıcı

[26] Mario Trujillo, "Firms That Sell Spy Tech to Iran Remain Elusive" The Hill, 13 Ocak 2016, http://thehill.com/policy/technology/265760-firms-that-provide-spy-tech-to-iran-remain-elusive

[27] Arta Shams, "The State of Surveillance in Iran's Cyberspace" Azad Tribune, 14 Mayıs 2015, https://www.article19.org/azad-resources.php/resource/37964/en/the-state-of-surveillance-in-iran%E2%80%99s-cyberspace

[28] Golnaz Esfandiari, "Iran's Cyberpolice Call on Internet Giants to Prevent 'Crime' Amid Telegram Concerns" Radio Free Europe Radio Liberty, 5 Eylül 2015, http://www.rferl.org/content/iran-cyberpolice-internet-giants-privacy-concerns/27228394.html

[29] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," Kasım 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf

adlarını, soyadlarını, baba adlarını, kimlik numaralarını, posta kodlarını ve telefon numaralarını almaları için bir yasal çalışma başlatmıştır[30]. Nükleer uzlaşma antlaşmasının imzalanması ve ekonomisinin açılmasıyla birlikte İran, ilave tehditlerle karşı karşıya kalmaya ve İnternet ve dijital teknolojinin neredeyse 80 milyonluk nüfusu için artan önemine şahitlik etmeye mahkumdur.

AB - ABD GİZLİLİK KALKANI ANLAŞMASI

16 Ekim 2015 tarihinde Avrupa Toplulukları Adalet Divanı'nın (ATAD) Maximilian Schrems v. Veri Koruma Komiseri davası, 2000 yılından beri AB ve ABD işletmelerinin sınırlar ötesi kişisel veri transferini düzenleyen ABD-AB Güvenli Liman Antlaşması'nı iptal etmiştir. ATAD, ABD firmalarının Avrupa standartlarına denk düşecek oranda yeterli veri koruması sunmadığı kararını vermiş ve "kamu kurumlarının düzenli olarak elektronik haberleşmenin içeriğine erişimine imkân sağlayan yasaların temel bir hak olan özel hayatın gizliliğinin özünü ihlal ettiği değerlendirmesi yapılmalıdır"[31] sonucuna varmıştır. Bunun yanı sıra Divan, yasal tazmin düzenlemelerinin olmamasının "etkili adil koruma temel hakkının özünü [ihlal ettiğine]"[32] karar vermiştir.

2 Şubat 2016 tarihinde, Güvenli Liman Anlaşmasının geçersiz kılınmasından yaklaşık dört ay sonra, Avrupa Komisyonu ve ABD, Atlantik ötesi veri akışlarına gizlilik çerçevesi sağlayan AB-ABD Gizlilik Kalkanı üzerinde uzlaşmış ve Güvenli Liman anlaşması çöpe atıldıktan sonra binlerce firmanın sıkışıp kaldığı adli bilinmezliğe dair kaygıları yatıştırmışlardır.[33] Yeni Gizlilik Kalkanı Antlaşması'nın iki ana teması vardır: arttırılmış gizlilik koruması ve yasal başvuru mekanizmaları. Artık ABD firmalarının ve istihbarat kurumlarının AB vatandaşlarının kişisel verilerini, özellikle "ABD Ticaret Bakanlığı ve Federal Ticaret Komisyonu'nun, Avrupa Veri Koruma Otoriteleri ile artan işbirliği vasıtasıyla da birlikte, daha sağlam denetleme ve yürütme sağlaması"[34] ile korumak yönünde daha büyük sorumlulukları vardır. Yeni Atlantik ötesi veri transferi antlaşmasıyla ABD kamu kurumları artık "Avrupalıları kitle halinde veya ayrım gözetmeksizin gözetlemeyeceklerinin" ve AB

---

[30] Saeed Kamali Dehghan, "Iran clamps down on Internet use" The Guardian, 5 Ocak 2012, http://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use

[31] Avrupa Birliği Adalet Divanı, "The Court of Justice declares that the Commission's US Safe Harbour Decision is Invalid" (Press Release No. 117/15), 6 Ekim 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[32] A.g.e.

[33] Avrupa Komisyonu, "EU Commission and the United States agree on a new framework for transatlantic data flows: EU-US Privacy Shield," 2 Şubat 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm

[34] A.g.e.

vatandaşlarının verilerine ulusal güvenlik ve suçla mücadele amacıyla erişilmesinin "açık koşullar, kısıtlamalar ve denetlemeye maruz olacağı ve genel erişimi engelleyeceğinin"[35] teminatını vermiştir. Diğer bir deyişle, ABD veri gizliliği standartları, ABD firmaları Avrupa'da faaliyet göstermeye devam etmek istiyorsa, AB'nin daha sıkı veri güvenliği standartlarına uyum göstermelidir.

Gizlilik Kalkanı Antaşması'nın ikinci önemli sonucu, kişisel verilerin korunmasına dair yükümlülüklerini ihlal eden ABD firmalarını şikâyet etmek isteyen AB vatandaşları için yasal başvuru mekanizmalarının yaratılması olmuştur. Böylelikle, AB vatandaşları kişisel verilerinin gizliliği konusunda şikâyet ve sorgulamalarını resmi olarak iletme fırsatını ilk kez bulmuştur. Bu şikâyet ve sorgulamaları Avrupalı ulusal veri koruma yetkilileri tarafından ilgili otoritelere iletilir ve Alternatif Uyuşmazlık çözümü ücretsiz olarak sağlanır. Dahası, ABD firmalarının şikayetlere yanıt vermek için zaman sınırlamaları vardır, bu da bireylerin uzun ve masraflı yasal mücadelelere takılıp kalmayacağını temin etmektedir. Gizlilik Kalkanı Anlaşması'nın uygulanmasının izlenebilmesi için Avrupa Komisyonu, ABD Ticaret Bakanlığı ve ABD ve Avrupa veri koruma otoritelerinden davet edilen ulusal istihbarat uzmanlarından oluşan ortak yıllık değerlendirme kurulu oluşturulacaktır.

AB üyeliğine aday sıfatıyla, Türkiye'nin veri korunması ve gizliliğine dair yasal çerçevesi ve uygulamalarının AB standartlarıyla uyumlu olması gerekmektedir. Bu açıdan Ocak 2016 itibariyle başlayan Kişisel Verilerin Korunması Kanun tasarısı ile ilgili yasama çalışması bir dönüm noktası olmaya adaydır.

TÜRKİYE'NİN KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISININ DEĞERLENDİRMESİ

Türkiye'ye özgü bir veri koruması kanunu ilk olarak 2003 senesinde, AB Katılım Ortaklığı Belgesi konu ile ilgili bir maddeye değindiğinden dile getirilmiştir. Bu madde daha sonra Türkiye'nin AB Katılım Ulusal Programına kabul edilmiş ve Türkiye'de bir veri koruması yasa taslağının oluşturulmasının ilk denemelerinden biri 2008'de olmuştur. Ancak veri korunması konusunda kanun yapımının ivme kazanması, ancak Aralık 2014'te Kişisel Verilerin Korunması Kanun tasarısı[36] oluşturulması ve ilgili AB kurumları ve yerel sivil toplum gruplarına yasal yorumları için iletilmesi ile gerçekleşmiştir. Yapılan değişiklikler

[35] A.g.e.
[36] Kişisel Verilerin Korunması Kanun Tasarısı. 18 Ocak 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf

yeniden düzenlenen ve Meclis'e 18 Ocak 2016 tarihinde sunulan kanun tasarısında yer almıştır.

"Kişisel Verilerin Korunması Kanun tasarısı"[37] öncesinde de bu türde verilerin toplanmasına ve kullanılmasına dair bazı kanunlar mevcuttur. Temel olarak 2010'da yapılan değişikliklerden sonra Türkiye Cumhuriyeti Anayasası[38] verilerin korunmasını kişisel hakların bir parçası olarak kabul etmiş ve devletin bu verileri kaydetme ve işleme yetisine kısıtlamalar getirmiştir. Anayasanın doğrudan konu üzerine olan maddeleri 17 sayılı (kişinin dokunulmazlığı, maddi ve manevi varlığının genel olarak tanınması) ve 20 sayılı ("kişisel verilerin korunmasını isteme" hakkının ve bu verilerin düzeltilmesi ve silinmesi hakkının tanınması) maddelerdir. Diğer yandan Türk Medeni Kanunu'nda[39] 23, 24 ve 25. maddeler kişisel hakları korumaktadır; ancak bunlar doğrudan çevrimiçi kimliklere veya veri haklarıyla ilgili değillerdir. Türk Borçlar Kanunu[40] (Kanun No. 6098) veri kullanımının mali boyutuyla ilgilenmekte, 419. Maddesi işverenleri çalışanlarının performans ve niteliklerine dair kişisel verileri korumakla yükümlendirmektedir. Son olarak Ceza Kanunu'nda[41] özel verilerin gizliliğinin ihlal edilmesi üzerine 134 sayılı, verilerin yasa dışı kaydedilmesi, veri toplama kanununun ihlal edilmesi, rıza dışında veri toplanması üzerine 135 sayılı, kişisel verilerin transfer ve dağıtımı üzerine 136 sayılı ve veri yok etme politikası ve yok etmeme üzerine 138 sayılı maddeler mevcuttur. Bunun yanı sıra Bilgi Edinme Hakkı Kanunu[42], bazı kurumsal, kişisel ve devlet verilerine bir miktar erişim sağlamaktadır; gizli verilere erişim ise açıkça kısıtlanmaktadır.

Ayrıca, sektöre özel kanunlar da mevcuttur. Bunların arasında, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik ve İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, e-Ticaret Yasası, Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik, Banka ve Kredi Kartları Kanunu, Mesafeli Sözleşmeler Yönetmeliği ve Elektronik Haberleşme Kanunu ile ikincil mevzuatı gelmektedir.

---

[37] Kişisel Verilerin Korunması Kanun Tasarısı. 18 Ocak 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf

[38] Türkiye Cumhuriyeti Anayasası. https://www.tbmm.gov.tr/anayasa.htm

[39] Türk Medeni Kanunu #8049 http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.4721&MevzuatIliski=0&sourceXmlSearch

[40] Türk Borçlar Kanunu. #10757 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf

[41] Türk Ceza Kanunu. #8965 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

[42] Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik. BDDK. http://www.bddk.org.tr/websitesi/turkce/bize_ulasin/454bilgi_edinme_yon.htm

Türkiye'nin veri gizliliği kanununun ilk taslağını uluslararası normlar açısından değerlendiren Nurullah Tekin, Türkiye'nin Avrupa Konseyi, Birleşmiş Milletler ve OECD üyesi olmasına rağmen, "bu kurumlar tarafından veri korunması hakkındaki prensipleri kendi milli mevzuatına dâhil etmekte başarısız olduğunu" belirtmiş ve "Türkiye'nin hala kişisel verilerin işlenmesi konusunda açık ve yeterli yasal düzenlemelerinin olmadığı"[43] sonucuna varmıştır. Tekin aynı makalede Avrupa Konseyi'nin Türkiye raporlarında, bu yönde bir kanunun yokluğuna büyük bir eksiklik olarak değindiğini ve bu yokluğun aynı zamanda Türkiye'nin 23 (Yargı ve Temel Haklar), 24 (Adalet, Özgürlük ve Güvenlik), 10 (Bilgi Toplumu ve Medya) ve 28 (Tüketicinin ve Sağlığın Korunması) fasıllarında ilerlemesini etkilediğini vurgulamaktadır. Buna ek olarak, 19 Ocak 2015[44] tarihli TÜSİAD görüş raporu, belirli bir veri koruması yasasının olmamasının Türk ve Avrupalı iş ve yatırım faaliyetlerinin, iş, çalışan ve yatırım verisinin yasal uyuşmazlıklar durumunda nasıl işleneceğine dair açıklar ve yasal boşluklardan ötürü uyumlaştırılmasını zorlaştırdığını vurgulamıştır.

Ancak böyle bir kanuna olan ihtiyacın değerlendirilmesinde yasal kaygılardan öte siyasi kaygılar kritik rol oynamıştır. Öncelikle Türkiye'ye mülteci sorunuyla başa çıkması için verilen birkaç milyar Euro'luk yardım paketi, Türkiye-AB ilişkileri için bir itici güç olmuş, buna veri transferleri konusunda işbirliği de dâhil olmuştur. EUROJUST ve EUROPOL verilerinin Türkiye ve AB arasında mülteci akışı politikasını koordine etmek için transfer edilmesiyle alakalı olduğundan, kişisel verilerin korunmasının sınırlarını açıkça çizen bir yasanın varlığına ihtiyaç acil hale gelmiştir. Ancak taraflar bundan da önce, Schengen bölgesine seyahet edecek Türk vatandaşlarına vize muafiyeti sağlayacak Türkiye ve AB Vize Serbestisi Diyaloğu Aralık 2013'te başlatmıştır. Vize Serbestisi Diyaloğunda yetmiş iki teknik maddenin iki tanesi veri koruma konusu ile doğrudan ilintilidir. Hâlihazırda Avrupa İstikrar İşbirliği adlı düşünce kuruluşu Türkiye'nin Vize Serbestisi Diyaloğu[45] konusundaki performansının çevrimiçi bir karnesini tutmaktadır. Bu karnede Türkiye'nin bu alanlardaki statüsü '5' (en düşük puan)'tir.

KANUN TASARISININ DEĞERLENDİRMESİ

[43] Tekin, N. 'An Assessment of the Turkish Draft Law on Protection of Personal Data in Light of the EU Data Protection Directive'. *Human Rights Review*, Cilt:IV, Sayı:1, Haziran 2014

[44] 'Kişisel Verilerin Korunması Kanunu Tasarısı Hakkında TÜSİAD Görüşü'. http://www.tusiad.org.tr/__rsc/shared/file/Kisisel-Verilerin-Korunmasi-Kanunu-Tasarisi-Hakkinda-TUSIAD-Gorusu.pdf

[45] Turkey's Visa Liberalization Roadmap. European Stability Initiative. 17 Aralık 2014. http://www.esiweb.org/index.php?lang=en&id=555

Kişisel Veri Koruma Kanun tasarısında belirtilen kişisel veri, "bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak tanımlanabilir. Bu bağlamda kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgiler, kişisel veri olarak nitelendirilmektedir"[46]. Tasarının çıkış noktası, kayıtların fişleme için kullanıldığı düşüncesinin önüne geçmektedir. Ayrıca Kanun, mevcut yasal sistemin, kişisel verilerin kamu ve özel sektör tarafından suistimal edilmesini engellemediğini, bu verileri kimin topladığı ve nasıl işlediğine dair belirsizlik olduğunu öne sürmektedir. Daha pratik, hatta kanun tasarısının zamanlaması için daha önemli olarak, mülteci krizinin mevcut boyutundan önce gelen gerekçe, Türk polisi ve EUROPOL arasındaki ilişkinin güçlendirilmesi gerekliliğine işaret etmektedir. Mülteci probleminin aldığı mevcut boyut söz konusu olduğunda, Türk Polisi ve EUROPOL arasındaki ilişki, özellikle mültecilerin işleme tabi tutulurkenki veri paylaşımı açısından, hiç olmadığı kadar önemlidir. Kanun tasarının temel gerekçelerinden biri, Türkiye'nin Avrupa Birliği kişisel veri koruma koşullarına uymayışından kaynaklanan, Türk ve Avrupa polis merkezlerinin veri transferi ve işbirliği alanlarındaki eksikliğidir. Buna ek olarak gerekçe, EUROJUST yetkisi altında yer alan, Türkiye'de meydana gelen ya da transit geçen suç faaliyetlerindeki artışa dikkat çekmekte ve veri gizliliği çercevesinin olmayışının, şuç verilerinin etkin paylaşımını engellediğini savunmaktadır.

EDAM'ın değerlendirmesine göre, asıl amacın Türkiye'deki Veri Koruma Kanunu'nu AB müktesebatı ile uyumlaştırmak olduğu bu çerçevede, kanun tasarısının iki temel sorunu vardır. Bunlardan ilki, kanun tasarısının Veri Koruma Kurulu'nun bağımsızlığına ilişkin şüphelerdir. İkinci problem ise, kişisel verilere erişim ile ilgili kamuya tanınan geniş istisnalardır. Bu, Amerikan istihbarat kurumlarının AB-kökenli kişisel verileri nasıl işleyeceklerine dair açık ve kesin sınırlamalar koyan AB-ABD Gizlilik Kalkanı Antlaşması sonrasında daha fazla önem taşımaktadır. Bunun AB'nin Türkiye'deki yasal düzenlemeye dair beklentilerine yansıması kaçınılmazdır.

Tablo 1 – Türk Kanun Tasarısına Bir Bakış

Kişisel Verilerin Tanımlanması	Kişisel kimliği, iletişim bilgilerini, sağlık ve mali bilgiler, dini, özel ve siyasi görüşleri belirli hale getirebilecek her tür bilgi.

[46] Kişisel Verilerin Korunması Kanun Tasarısı. 18 Ocak 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf

Kanunun Gerekçesi	Kişisel verilerin kullanımının özel sektör ve kamu sektörü tarafından istismar edilebilmesi. Bu verilerin yetkisiz bireyler tarafından kullanılması ifşalara, istismara ve Anayasa ile Türkiye'nin taraf olduğu uluslararası sözleşmelerin ihlaline yol açabilmesi. Ticari faaliyetleri kolaylaştırmak için verilerin sınırsız akışı ile bu verilerin istismar edilmesinin önlenmesi arasında makul bir yasal denge oluşturulması gereksinimi. Kişisel verilerin kullanımı ve işlenmesi üzerine yasal dayanak ve denetim mekanizması olmamasının bu tür verilerin kullanılması konusunda genelgeçer bir şüpheye yol açması. Türk veri koruma kanunlarını gelişmiş ülkelerin yasalarıyla uyumlu hale getirme ihtiyacı. Türkiye güvenlik birimleri ve EUROPOL arasında polis ve güvenlik işbirliği ve istihbaratın elektronik transferi konularında uyumluluğun sağlanması için yeni yasa ihtiyacı. Benzer şekilde istihbarat paylaşımı konusunda yasal çerçevenin uyumsuzluğu sebebiyle EUROJUST ile koordinasyonun zedelenmesi ve bunun ortak mücadele operasyonlarını engellemesi. Sağlık kurumları tarafından toplanan kişisel verilerin artan miktarının gittikçe sorunlu hale gelmesi ve bu kurumların veri saklamak için yasal temelleri veya yeterli güvenlik çerçevelerinin olmaması. AİHS'nin bu boşluğu kişisel gizliliğin ihlali olarak değerlendirmesi. Yurtdışında yaşayan Türk vatandaşlarının, askerlik durumu, vatandaşlık ve mali varlıkları konusundaki bilgilerinin paylaşımıyla ilgili sorunların olması ve bunun, Türkiye'deki yasal durumlarını karmaşıklaştırması. Kişisel veri kullanımı kanunundaki yetersizliklerin doğrudan yabancı yatırımların ve Türkiye içindeki yabancı anaparanın yönetimine zarar vermesi. Bu yasal boşlukların yatırımcıların Türkiye'deki yatırım ve ticari faaliyetlerini geliştirmesini caydırması ve Türk işadamlarının yurtdışına iş ortaklıkları kurmasını kısıtlaması.
Mevcut Yasal Çerçeve	5237 Sayılı Türk Ceza Kanunu Madde 135: Kişisel verilerin hukuka aykırı toplanması ve ifşası Belirlenen Problem: Bu eylemlerin ne zaman yasal ve yasadışı olduğu

	konusuna yasal açıklık ve karışıklık. Anayasa Değişikliği (2010 Referandumu) Madde 20: Kişisel verilerin korunması temel bir insan hakkı sayılır. Avrupa Birliği Katılım Çerçevesi: Katılım Müzakerelerinin Dört Faslı kişisel verilerin korunmasıyla alakalıdır. Bu dört fasılda ilerleme kaydedilmesi için yeni, konuya özel bir yasaya ihtiyaç vardır. Kişisel verilerin korunması Türkiye'nin AB Katılım Ortaklığı Belgesine 2003'te verdiği yanıtta vadedilmiştir. 64. Hükümet Programı bir Acil Eylem Planı yayınlamış, planda kişisel verilerin korunması reformunun üç ay içerisinde gerçekleştirilmesi vadedilmiştir. Türkiye OECD'nin 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelerine taraftır. Türkiye Avrupa Konseyi'nin 1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine (CETS No. 108) taraftır. Türkiye Avrupa Parlamentosu ve Konseyi'nin 24 Ekim 1995 tarihli, bireylerin kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımına karşı korunması 95/46/EC Direktifine taraftır.

Eski versiyonlarda yer almayan, "açık rıza" koşulu (Madde 3/b), yeni kanun tasarısının en temel değişikliklerindendir. Bu yeni kanun, kişisel rızaya ve rızanın ifade edilmesinin kişisel veri işlenmesinin temeli olduğuna üstü kapalı bir şekilde dikkat çekmektedir. Açık rıza koşuluna karşı aşağıdaki durumlar istisna olarak belirtilmiştir (Madde 5):

a) Çakışan bir yasa bulunması,
b) Fiziksel zorluk ya da rızanın ifade edilmesi üzerindeki yasal sınırlamalar sebebiyle, ya da kişisel veri işlenmesinin bireyin veya başkasının fiziksel güvenliğini korumak için gerekli olduğu durumlarda - bireyin rızasını ifade etme yetersizliği,
c) Kişisel veri işlenmesinin başka bir antlaşma ya da kontratı yaratmak ya da uygulamak için gerekli olduğu durumlarda,
d) Sorumlu yetkili yasal olarak kişisel veri işlenmesi yapmakla yükümlü olduğunda,
e) Kişisel veri birey tarafından ifşa edildiği ya da halka açık hale getirildiğinde,
f) Kişisel veri işlenmesi başka bir hakkı yaratmak, uygulamak ya da savunmak için gerekli olduğunda,
g) Kişisel veri işlenmesinin veriyi işleyen yetkili bireyin, temel hak ve özgürlüklerinin ihmal edilmediği taktirde, meşru çıkarları için gerekli olduğu durumlarda.

Bu anlamda yasa, kişisel verinin korunmasına pek çok koşul ve sınırlama getirmektedir. Madde 5'in maruz kaldığı ana eleştirilerden biri, her ne kadar yasanın gerekçeleri arasında tam tersi yer alsa da, yeni yasanın uluslarası antlaşmalar ya da AB hukuku ile uyumsuz olduğudur. Buna ek olarak, yukarıda belirtilen istisnai durumlar yeni yasayı fazlaca kısıtlamakta ve onu mevcut Türk yasal sistemi içerisinde AB kurumlarınca, daha iyi veri akışı yönünden yetersiz olarak sınıflandırılabilecek bir konuma yerleştirmektedir.

Yeni taslağın 6. Maddesi, Gizli Kişisel Bilgi (PPI) ve diğer hassas verilere istenilen özgürlükler kapsamında başkaca sınırlamalar getirmektedir. Madde kişisel verileri, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, cezai ve biyometrik verileri olarak tanımlamakta[47] ve bu verilerin yeterli güvenlik tedbirleri ya da bireyin rızası olmadan işlenemeyeceğini belirtmektedir. Ancak tasarının 5. Maddesi, hassas bilgilerin işlenmesine dair aşağıdaki durumlar söz konusu olduğunda başkaca sınırlamalar getirmektedir:

a) Başka bir yasanın hassas verileri işlemesi gerektiğinde,
b) Verinin işlenmesinin derneğin çalışma alanlarıyla kesin surette alakalı olduğu şartıyla, siyasi partilerin, sendikaların, derneklerin ya da diğer kar amacı gütmeyen organizasyonların uluslarası yasaları gereğince hassas verileri işlemesi gerektiği durumlarda,
c) Hassas verinin söz konusu birey tarafından halka açık ya da erişebilir hale geldiği durumlarda,
d) Hassas veri işlenmesinin başka bir hakkı yaratmak, uygulamak ya da savunmak için gerekli olduğu durumlarda,
e) Bu işlemenin, halk sağlığının korunması, önleyici tıp, tıbbi teşhis, tedavi ve bakım gibi sağlıkla alakalı aktivitelerin sır yemeni etmiş kurumlar ve bireyler tarafından planlaması, idaresi ve finansmanı için kullanıldığı durumlarda.

Tasarı kişisel verilerin geri alınması, silinmesi ve anonimleştirilmesi faaliyetlerini de kapsamaktadır (Madde 7) ancak bu konuda uygulamada önem taşıyacak birçok önemli ayrıntının daha sonra yönetmelikler yolu ile belirginlik kazanacağını ifade etmektedir. Benzer bir sorun, kişisel verilerin üçüncü taraflarla paylaşılmasını yasaklayan 8. Madde'de de görülmektedir; ancak 6. Madde'de deki istinai durumlar ('b' hariç) bu madde için de geçerlidir.

[47] Kişisel Verilerin Korunması Kanun Tasarısı. 18 Ocak 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf

Madde 10, 11 ve 12 veriyi işleyen yetkili partiye, kişisel veri kapsamında başkaca görevler ve haklar tanımaktadır. 10. Madde'ye göre, veri yetkilisi şunları temin etmekle yükümlüdür:

a) Kişisel verisi işlenecek bireyin verisini işleyecek olan yetkili bireyin kimliği,
b) Söz konusu verinin işlenme amacı,
c) Söz konusu verinin kimlerle ve hangi sebeplerle üçüncü partilere aktarılabileceği,
d) Veri toplamanın yöntemi ve hukuki temeli,
e) Kişisel verisi toplanacak bireyi, Madde 11'de öngörülen diğer hakları konusunda bilgilendirmek.

Madde 11 gereğince kişisel verileri işlenen kişinin hakları olarak belirtilen haklar aşağıdaki gibidir:

a) Kişisel verilerinin işlenip işlenmediğini öğrenme,
b) İşlenmişşe buna ilişikin detayları talep etme,
c) Verilelerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
d) Verilerin aktarıldığı üçüncü partileri bilme,
e) Verilerin eksik ya da gerçeğe aykırı olması hallerinde bunların düzeltilmesini isteme,
f) 7. Madde'de öngörülen koşullar çercevesinde kişisel verilerin silinmesini veya yok edilmesini talep etme,
g) (e) ve (f)'de belirtilen değişiklikler durumunda üçüncü partiyi bilgilendirme,
h) Otomatik sistemler aracılığıyla işlenen kişisel verilerde ortaya çıkan olumsuz etkilere karşı çıkma,
i) Kişisel verilerin kanuna aykırı işlenmesi sebebiyle zarara uğrası halinde, zararın giderilmesini talep etme.

Bunu takiben yer alan Madde 12, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek ve gerekli her türlü tedbiri almak gibi maddeleri kapsayarak, veri sorumlusunun yükümlülüklerini düzenlemektedir. Verilerin uygun olmayan bir biçimde ele alınması durumunda veri sorumlusu durumu, üst yetkili konumundaki Kişisel Veri Savunma Kurulu'na bildirmekle görevlidir.

Verilerin uygunsuz kullanıldığı durumlarda tasarı, hukuki şikayeti, 30 gün içerisinde cevap vermekle yükümlü ve gerektiği taktirde ek ücret talep edebilecek olan, veri sorumlusuna iletecektir. Ancak tasarı, bahsi geçen ücreti kimin talep edebileceği konusuna netlik getirmemektedir. Söz konusu uygunsuzluğun veri sorumlusundan kaynaklaması durumunda alınan ücret iade edilecektir. Şikayetin yalnızca veri sorumlusu tarafından reddedilmesi ya da cevapsız kalması hallerinde, ilgili kişi, hukuki telafi yetkisini elinde bulunduran Kurul'a

şikayette bulunabilir. Kurul, 15 gün içerisinde hazırlamakla yükümlü olduğu belgeler beraberinde veri sorumlusunu, kişisel veri işleme kapsamında yasal uygulamaya tabi tutarak, ve söz konusu verinin gerekli vakalarda uluslararası üçüncü partilere aktarılmasını kısıtlayarak, şikayete cevap vermek durumundadır.

Tasarının bir başka hassas boyutu, Verileri Koruma Kurulu'nun yapısının düzenlendiği bölümdür. Kurumun, özel ve kamu sektöründe en az 10 yıllık tecrübesi ve 4 yıllık lisans diploması olan yedi üyeden oluşması öngörülmektedir. Kurumun en kritik noktası, 4 üyesinin Bakanlar Kurulunca 3 üyesinin ise Cumhurbaşkanınca atanmasıdır. Oysa ki 2014 tasarısında, en az 10 senelik hukuki tecrübesi olan 2 hakim veya avukat, en az 10 senelik yüksek eğitim tecrübesi olan 1 akademisyen ve Bakanlar Kurulunca, özel ya da kamu sektöründe en az 10 yıllık tecrübesi olması şartıyla, atanacak 4 üyeden bahsedilmektedir. Önerilen yöntem, AB standartlarına uyum açısından da kritik noktalardan biri olan Kurul'un yürütme erkinden bağımsızlığı konusunda tereddüt yaratmaktadır.

Kanun tasarısının 2014 ve 2016 olmak üzere her iki versiyonunu itibariyle de ortaya çıkan bir diğer sorun, muhtelif gerekçelerle kamuya ve kamu kurumlarına tanınan kişisel verilere erişimlerini kolaylaştıran istisnalardır. "Milli güvenlik" ve "önleyici, koruyucu ve istihbarat aktiviteleri" hususları tasarıya işlemiş olan istisnalardan bir kaçıdır. Bu istisnaların genel ve açık olmayan tanımlamalarısöz konusu terimlerin çok geniş bir yelpazede ele alınması riskini yaratmaktadır. Her ne kadar güvenlik hususları AB müktesebatında önemli bir takım meşru istisnalar olarak yer alsalar da, mevcut kanun tasarısı çevrimiçi ifade özgürlüğü ve gizliliği ve milli güvenlik arasındaki doğru dengeyi bulmakla yükümlüdür. Nitekim ABD ile AB arasında kişisel verilerin transfer edilmesine olanak sağlayan Güvenli Liman – Safe Harbor anlaşması tam da bu nedenle ATAD tarafından iptal edilmiştir. Divan kararı ABD istihbarat kuruluşlarının kişisel verilere ulaşmalarına yönelik yeni bir düzenleme yapılması gerekmiş ve bunun sonrasında Avrupa Komisyonu ile ABD yönetimi arasında, ABD güvenlik ve istihbarat kurumlarının kişisel verilere erişimi daha fazla denetim alınmasını sağlayan Privacy Shield anlaşması müzakere edilmiştir. Uluslararası ortamda bu tip gelişmeler yaşanırken, Türkiye'nin yasama sürecindeki bu kanun tasarısının AB tarafından da benzer bir yaklaşım ile değerlendirileceğini söylemek gerekir.

POLİTİKA TAVSİYELERİ

- Kişisel özgürlükler ve gizlilikle alakalı olan maddelerdeki istisnalar AB düzenlemeleri ışığında yeniden ele alınmalıdır.
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi hakkı (Madde 7) daha açık olmalı ve yasal olarak daha iyi yapılandırılmalıdır.
- Kişisel Verileri Koruma Kurulu'nun önerilen yapısı gözden geçirilmelidir. Bakanlar Kurulu veya Cumhurbaşkanlığı haricinde akademi, yargı ve meslek kuruluşlarından da atama yapılmasının yolu açılmalıdır.
- Ulusal güvenlik kaygıları, özellikle Türkiye'nin hâlihazırda iç ve dış güvenlik açıklarıyla mücadele ettiği göz önüne alındığında, veri gizliliği çerçevesinden muafiyet/istisnalar için makul gerekçeler olabilir. Ancak son ABD-AB Veri Koruma Anlaşması'ndan da görülebileceği gibi, "ulusal güvenlik" kavramının sağladığı kişisel verilere erişim yetkisinin de daha belirgin bir denetim mekanizmasına tabi tutulması gerekmektedir.
- Tasarının bu şekliyle kabulü halinde temel risk, AB tarafından yapılacak değerlendirmede Türkiye'nin yasanın çıkmış olmasına rağmen kişisel verilerin transfer edilebileceği güvenli ülke sıfatını kazanamamısıdır. Bu durum zaten vize serbestisi konusunda ayak süremek isteyen bazı AB ülkelerine bekledikleri ve istedikleri gerekçeyi sağlaycaktır.
- Vize serbestiyeti sürecine zarara vermesinin ötesinde, AB standartlarına uymayan bir yasal düzenleme ile diğer hedeflere erişilmesi de mümkün olmayacaktır. Polisiye ve adli vakalarda EUROPOL ve EUROJUST ile veri değişimi gene yapılamayacaktır.
- Üstüne üstlük, Kişisel Verilerin Korunmasına dair bir yasal düzenleme ile yapılması ile bugüne kadar yurtdışına veri transfer edebilen ulusal ve uluslararası şirketler de bu düzenlemeye uyum sağlamakla mükellef olacaklardır. Ancak AB'nin Türkiye'yi veri korunması anlamında güvenli ülke tanımına sokmaması, Türkiye'den AB ülkelerine yapılacak veri transferlerine onay verilmesini de belirsizliğe atacaktır.