204

Ocak 2018

İKV DEĞERLENDİRME NOTU

AB VERİ GÜVENLİĞİ EKOSİSTEMİNİN YÖRÜNGESİNDEKİ TÜRKİYE'DEN NOTLAR

Ahmet CERAN
İKV Uzmanı

Melis BOSTANOĞLU
İKV Uzman Yardımcısı

İKTİSADİ KALKINMA VAKFI

www.ikv.org.tr

AB VERİ GÜVENLİĞİ EKOSİSTEMİNİN YÖRÜNGESİNDEKİ TÜRKİYE'DEN NOTLAR

Ahmet CERAN, İKV Uzmanı

Melis BOSTANOĞLU, İKV Uzman Yardımcısı

Popülizm kıskacında ve kurumsal geleceğine ilişkin buhranlı tartışmaların odağındaki AB, son yıllarda Üye Devletlerin mali krizleri ve küresel terör, mülteci krizi gibi sınamalarla tökezlemekte olsa da, bir alanda halen daha ulusal sistemdeki yönlendirici, dönüştürücü, kural koyucu rolünü sürdürüyor: dijital dönüşüm. Dijital Tek Pazar stratejisini bütün hukuki düzenlemeleriyle birlikte verimli şekilde hayata geçirmesi halinde AB ekonomisinin yıllık 416 milyar avro katma değere sahip olması ve yüz binlerce yeni istihdam sağlaması bekleniyor.[1] Böyle bir perspektifle bakıldığında, aynı strateji çerçevesinde Birlikle yakın ekonomik, siyasi ve sosyal ilişki içerisindeki ülkelerin de aynı modele ayak uydurabilmesi büyük önem taşıyor ki bu ülkeler arasında ilk sıralarda Türkiye geliyor.

Genel Tespitler

- **25 Mayıs 2018 tarihinde yürürlüğe girecek olan GDPR'ın AB ülkeleri kadar, AB ile siyasi/ticari etkileşim içerisindeki ülkelerde de yakından takip edilmesi gerekiyor.**
- **GDPR ve veri paylaşımı, dijitalleşen dünyada pek çok boyutuyla Türkiye-AB ilişkilerinin geleceği açısından başat bir rol taşıyor.**
- **Türkiye'de veri güvenliği reformuna yönelik atılan adımlar ve ulusal çapta bilgilendirme hamleleri; hem Türkiye'nin vizesiz Avrupa ülküsü için değerli hem de dijitalleşen küresel sistemin dinamiklerine ayak uydurabilmek için şarttı.**
- **Türkiye'de şirketlerin konuya ilişkin farkındalığının artırılmasında meslek kuruluşlarına, odalara ve borsalarla birlikte teknoloji odaklı sivil toplum kuruluşlarına önemli rol düşüyor.**
- **Türk yetkili makamların, vize serbestliği diyaloğunun hızlandırılması için Komisyona iletmeye hazırlandığı pozisyon belgesinde, veri güvenliği alanında öngörülen reform hamlelerinin doğru belirlenmesi gerekiyor.**

[1] Avrupa Komisyonu, "Digital single market, bringing down barriers to unlock online opportunities", https://ec.europa.eu/commission/priorities/digital-single-market_en

AB'nin bu büyük dijital dönüşüm hamlesinin odağında yer alan veri güvenliği reformu konusu, AB vatandaşlarının haklarını daha ileri seviyede korumayı hedefleyen yapısı; veri transferini daha etkin ve dijital ekonomiyle daha entegre hale getiren sistematiğiyle, özel bir önem taşıyor. Bu bağlamda AB veri güvenliği reformu, Nisan 2016 tarihinden beri olabildiğince hızlı şekilde dizayn ediliyor.

AB veri güvenliği reformunun temel unsurunu teşkil eden ve AB çapında tek hukuki düzenleme çerçevesinde bütün Üye Devletlerin ve kurumların veri güvenliği aynı standartlara bağlılığını zorunlu kılan Genel Veri Koruma Tüzüğü'nün (*General Data Protection Regulation* – GDPR) 25 Mayıs 2018 tarihinde yürürlüğe girecek olması ve o tarihten itibaren AB'de ve AB ile veri transferi yapacak tüm paydaşların bu kurallara uyması zorunluluğu, konunun azami önemini daha da katlıyor. GDPR, bir yandan AB'ye yönelik hantallık eleştirilerine istisna oluşturuyor diğer yandan da AB ile veri paylaşımını dijitalleşen dünyada pek çok boyutuyla Türkiye-AB ilişkilerinin geleceği açısından başat bir rol oynuyor. Dolayısıyla Türkiye'de de konunun pek çok açıdan yüksek sesle ve sık şekilde gündeme taşınması, AB veri güvenliği ekosisteminin güncel yapısının Türkiye'deki kamu, iş dünyası, akademi ve sivil toplum merkezli paydaşlar tarafından anlaşılır hale gelmesi gerekiyor.

AB Veri Güvenliği Ekosisteminin Evrimsel Gelişimi

Dördüncü sanayi devrimi tartışmalarıyla birlikte ekonomik süreçlerin merkezinde yer alan ve "yeni petrol" hatta yeni para birimi gibi görülen veri konusu aslında doğrudan temel hak ve özgürlüklerin korunmasıyla bağlantılı bir mesele.

AB Temel Haklar Şartı (*EU Charter of Fundamental Rights)*'nın 8'inci Maddesi, kişisel verilerin korunmasını, AB'nin yapısal çatısı olarak belirliyor ve sonrasındaki bütün müktesebat iyileştirme hamleleri de aynı mantığa dayanıyor. AB'nin konuya ilişkin öncelikli hukuki düzenlemesi, yerini GPDR'ın alacağı 1995 tarihli AB Veri Güvenliği Yönergesi'ydi. AB, 20 yıl boyunca Üye Devletlerin bu düzenlemeye uyumuna yönelik çalışmalarını sürdürürken kolluk kuvvetleri ve güvenlik işbirliği, ticaret, sağlık ve telekominikasyon alanında ikincil düzenlemelerle ekosistemi güçlendirmeye çalıştı.

2016 yılına gelindiğinde ise GDPR'la birlikte kolluk birimlerinin işbirliği alanına ilişkin bir yönergenin uzun müzakereler; AP, Konsey, Komisyon üçgeninde dişli tartışmalar sonucunda kabulüyle evrimsel gelişim hız kazandı. Genel saik ise çok basit: AB'yi oluşturan bütün unsurların ve AB ile ilişki içerisindeki tüm üçüncü ülke unsurlarının karşılıklı veri paylaşımı sağlayabilmesi için aynı oranda ileri seviye ve yeterli kişisel verilerin korunması standartlarının oluşturulması.

Güncel küresel sınamalar ile dijital dönüşümün beklenmeyen hızı ve yarattığı ekonomi; AB veri güvenliği ekosisteminin sınır yönetimi, göç kontrolü gibi alanlarda veri işbirliğini ve standardizasyonunu artırmaya yönelik EUROSUR, EURODAC gibi

çerçeveler, uçuş bilgilerinin paylaşımına ilişkin PNR Düzenlemeleri, vize operasyonlarını reforme etmesi beklenen AB Seyahat Bilgileri ve Yetkilendirme Sistemi (ETIAS) ve benzeri girişimlerle güçlenmesini sağladı.[2] Dolayısıyla bu evrimsel gelişimin ışığında, 25 Mayıs 2018 tarihinde, bahsi geçen serüveni bir sonraki aşamaya taşıyacak olan ve aslında AB ile birlikte tüm bağlantılı ülkelerin heyecanla beklediği GDPR'a daha yakından bakmak gerekir.

Genel Veri Koruma Tüzüğü (GDPR) Kullanıcılara Neler Getiriyor?

Dünyanın her geçen gün daha da dijitalleşiyor olduğu ve bu dijitalleşme sonucunda internetin de ticarileşme yolunda önemli bir araç haline geldiği düşünüldüğünde; AB tarafından 1995 yılında uygulamaya koyulan AB Veri Güvenliği Yönergesi, bugünün sorunlarını çözmekte pek de yardımcı değil.

Özellikle Yönerge'nin her üye ülkede farklı yorumlanmasının gerçek kişilerin verilerinin korunmasının önünde engeller teşkil ettiği gerçeği de veri güvenliği alanında reform gerekliliğinin habercisiydi. Gizliliğin (*privacy*) AB hukukunda sahip olduğu önem ve konum nedeniyle, daha kesin ve kapsayıcı kuralların oluşturulması, kaçınılmaz bir hal alıyor. Avrupa Komisyonu, Ocak 2012'de daha tutarlı ve kapsamlı bir koruma vadeden Genel Veri Koruma Tüzüğü taslağını ortaya koymuş, 2016 yılının nisan ayında bu taslak AP üyeleri tarafından onaylanmış, aynı yılın mayıs ayında ise AB Resmi Gazetesi'nde yayımlanmıştı.

Komisyonun 2015 ve 2016 yıllarında veri güvenliği hakkında yürüttüğü anketler de müktesebatın revize edilip, daha iyi hale getirilmesinin ne kadar büyük bir önem taşıdığının kanıtı niteliğinde. 2015 yılında veri güvenliğine ilişkin AB vatandaşlarının algısını ölçen Eurobarometre anket çalışmasının en önemli bulguları, katılımcıların çoğunun verilerinin güvenliğinden endişeli olduğunu, bundan dolayı da verilerinin hâkimiyetini kendi ellerine almak istediklerini gösteriyordu[3]. Ayrıca büyük bir çoğunluk, Birlik dahilindeki tüm ülkelerin veri güvenliği mevzuatı kapsamının aynı olmasından yanaydı. Bunun yanı sıra 2016 yılında ePrivacy Tüzüğü'ne hazırlık amaçlı yapılan ankette de benzer sonuçlar görebiliyoruz. [4] Bu ankette de, çevrimiçi gizlilik, özellikle de

[2] Avrupa Komisyonu, Smart Borders, Ocak 2018, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en Erişim Tarihi: Ocak 2018

[3] Eurobarometer, "Data Protection Report", Haziran 2015, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf Erişim Tarihi: Ocak 2018

[2] Eurobarometer, "e-Privacy Report", Aralık 2016, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76377 Erişim Tarihi: Ocak 2018

iletişimin gizliliği, internet üzerinden izin/onay gerektiren çerezleri takip etme, istenmeyen e-posta ve pazarlama çağrıları gibi anahtar meseleler çerçevesinde bir takım sorular sorulmuş, önemli cevaplar alınmıştı.

Temel bulgulardan bazıları şöyle:

- **Cep telefonları, aramalar ve kısa mesajlar için günlük olarak kullanılırken, internet üzerinden telefon konuşmaları ve video çağrıları genellikle ayda birkaç kez yapılıyor.**

  Cep telefonundan telefon görüşmeleri ve mesajları; internete çevrimiçi göz atma ve e-posta kullanımı; kullanıcılar tarafından günlük veya neredeyse günlük olarak en sık kullanılan hizmetlerden birkaçı. Kullanıcılar aynı zamanda interneti, haftalık olarak anlık mesajlaşmak ve çevrimiçi sosyal ağları kullanmak için kullanıyor.

- **Katılımcıların çoğu için kişisel bilgilerinin, çevrimiçi iletişimlerinin ve çevrimiçi davranışlarının gizliliği çok önemli.**

  Katılımcıların çoğu, kanunlara göre elektronik cihazlarındaki kişisel bilgilerin ancak izin verdiklerinde erişilebileceğinden veya kimsenin izinleri dışında cihazlarında bilgi depolayamayacaklarından haberdar, aynı zamanda bu hususun onlar için çok önemli olduğunu açıkça belirtiyor.

- **Katılımcıların, e-Privacy Tüzüğü'nün anlık mesajlaşmalarının ve çevrimiçi sesli görüşmelerinin gizliliğini güvence altına almadığından haberdar olma oranı çok düşük.**

  Katılımcıların çoğu, kanunlara göre elektronik cihazlarındaki kişisel bilgilerin ancak izin verdiklerinde erişilebileceğini veya kimsenin izinleri dışında cihazlarında bilgi depolayamayacağını bilse de, e-Privacy Tüzüğü yürürlüğe girmeden önce de anlık mesajlaşma ve çevrimiçi sesli görüşmelerin gizli olduğu ve izinleri olmadığı sürece kimsenin bunlara erişemeyeceği gibi yanlış bir kanıya sahip.

Sonuçlara bakılacak olursa, vatandaşlar sıklıkla kullandıkları internette kendilerini yeteri kadar güvende görmüyorlar. Bu da demek oluyor ki, AB'nin hazırladığı GDPR'ın yürürlüğe girmesi büyük bir önem arz ediyor. Aynı zamanda uzmanların yorumları, yapılan kamuoyu araştırmaları ve sektör temsilcilerinin değerlendirmeleri ışığında görülüyor ki, vatandaşlar mevcut mevzuatın ve GDPR'ın kapsamından pek haberdar değil, bu da onların bazı yanlış kanılara varmalarına neden oluyor. Zira 25 Mayıs 2018 gibi yakın bir tarihte yürürlüğe girecek olan mevzuatı ve tüm tarafların bu süreye kadar hak/sorumluluklarını öğrenmeleri çok önemli. Tüzüğün getirdiği haklardan bazıları:

1. **Üye Devletlerdeki Mevzuatın Uyumlaştırılması**
   1995 yılında yürürlüğe giren Yönergenin en büyük sorunlarından biri de üye ülkelerin ilgili düzenlemeleri kendi iç hukuk kurallarına göre yorumlamalarıydı. Bu da demek oluyor ki veri ihlallerine toleransı olmayan Üye Devletler ile bu konuda daha yumuşak kurallara sahip Üye Devletlerin ihlal dâhilinde çok farklı yaptırımlar uygulaması, bazı haksızlıklara yol açıyor. Yönetmeliklerin aksine GDPR, tüm üye ülkelere doğrudan uygulandığı için tüm üye ülkeler aynı hak ve yükümlülüklere sahip olacak. Böylece veri ihlali halinde her üye ülkede veri kontrolörleri, 20 milyon avro veya hizmet sağlayıcısının küresel gelirinin yüzde 4'ünü gözden çıkarmak zorunda.

2. **Şeffaflık**
   Veri işleme prosedürlerinin şeffaf, kısa ama öz, anlaşılabilir, kolayca ulaşılabilir bir şekilde, net ve yalın dille sunulması gerekiyor. Ayrıca Tüzüğe göre kontrolörlerin de veri sahibinin isteği doğrultusunda talep ettiği bilgiyi, en fazla bir ay içerisinde iletmesi gerekiyor.

3. **Kişisel Verilerin Nerede Toplandığı Hakkında Bilgi Alma Hakkı**
   Veri sahibinin, verilerinin nerede toplandığını öğrenmek istemesi durumunda kontrolör; sorumlu kontrolörün veya gerektiği takdirde kontrolör temsilcisinin kimliğini ve iletişim bilgilerini, veri koruma görevlisinin iletişim bilgilerini, kişisel verilerin işlenme amaçları ve hukuki dayanaklarını, verilerin üçüncü bir ülkeye ya da uluslararası bir organizasyona verilip verilmeyeceğini, verilerin nerede saklanacağını ve daha önce planlanandan farklı amaçlarla veri işlenmesi gerektiğinde bu bilgileri veri sahibine tedarik etmek zorundadır.

4. **Veriye Erişim Hakkı**
   Veri sahibinin ona ait olan verilerin işlenip işlenmediğini, eğer işleniyorsa bu verilerin; hangi amaçla işlendiği, kategorileri, kime verileceği, mümkünse ne kadar süreyle depolanacağı, mümkün değilse bu süreyi belirleyen kriterlerin neler olduğu; kişisel verilerin veri sahibinden alınmadığı durumlarda, kaynağın neresi olduğu bilgilerini öğrenme hakkı vardır.

5. **Verilerin Düzeltilmesi Hakkı**
   Hakkında yanlış veri bulunması durumunda veri sahibi, bu verinin düzeltilmesini isteme hakkına sahiptir. Ayrıca, veri işlenmesinin ifa edilme amacı da göz önünde bulundurulduğunda, veri sahibinin yarım kalmış bir veriyi tamamlama hakkı da bu tüzükle gelen haklardan biridir.

6. **Unutulma Hakkı**
   Veri sahibi, daha önceden paylaştığı verinin; mevcut durumlarda gerekli olmadığı kanısındaysa, işletilmesi iznini geri çekme kararı aldıysa veya kanunsuzca işlendiğini düşünüyorsa bu verinin silinmesini isteme hakkına sahiptir.

7. **Veri Taşınabilirliği Hakkı**
   Bu hak sayesinde veri sahibi verisini, saklayamaya yetkili olan kontrolörden başka bir kontrolöre taşıyabilir.

8. İtiraz Etme Hakkı

Veri sahibi, özel gerekçeleri olduğu sürece, istediği an kendisine ait kişisel verilerin işlenmesine itiraz etme hakkına sahiptir. Bu durumda kontrolör, veri sahibinin çıkarlarını, hak ve özgürlüklerini hükümsüz kılacak meşru dayanaklara sahip olmadığı sürece, söz konusu kişinin verilerini işleyemez.

9. Veri İhlali Dâhilinde Yetkili Otoriteye ve Veri Sahibine Bildirim

Veri ihlali durumunda veri işlemcisinin kontrolörü; kontrolörün ise 72 saat içerisinde bu ihlali Denetleyici Otoriteye bildirme zorunluluğu vardır. Bildirimin gerekçe olmadan yapılmaması halinde söz konusu olan kurum yaptırıma uğrar. Ayrıca kurum, veri ihlali durumunda veri sahibinin hak ve özgürlüklerini risk altına alıyor ise aynı şekilde bu durumu en kısa süre içerisinde veri sahibine bildirmekle yükümlüdür.[5]

Örnek Olay: UBER Sızıntıları

Son zamanlarda meydana gelen en büyük veri ihlallerinden biri hiç şüphesiz Uber adlı küresel çapta ün sahibi ulaştırma şirketinin, sahip olduğu sürücü ve müşteri verilerinin sızdırılmış olduğunu ve bu bilgilerin silinmesi karşılığında 100 bin dolara ulaşan meblağlar ödemek zorunda kaldığını bir yıl boyunca gizlemesiydi. Bu durumun Genel Verileri Koruma Tüzüğü'ne tabi bir AB'de yaşanmış olduğunu farz edecek olursak, şirketin yaptırıma uğramamak için 72 saat içinde bu ihlali bildirmiş olması gerekirdi. ABD'nin 48 eyaletinde veri ihlalini bildirmeye yönelik hukuki düzenlemeler bulunsa da, bunların yaptırım gücü yeterince yüksek değil. Dolayısıyla ABD'de de veri sızıntıları olduğunda en kısa sürede bilgilendirilmek isteyen senatörler, Federal Ticaret Komisyonu'nun şirketlerin verilerini güvende tutması için kritik protokoller oluşturdu.

10. Veri Paylaşım Kurallarının Sıkılaşması

Tüzüğe göre, kişisel verilerin üçüncü bir ülke veya uluslararası bir organizasyona transferi ancak, Komisyon söz konusu ülke veya uluslararası organizasyonun yeterli düzeyde koruma teminatı verdiği kanısında ise gerçekleşebilir. Bu da demektir ki, AB üyesi olmayan ülkeler, Üye Devletlerle dijital veri paylaşımı yapabilmek için GDPR' a benzer standartlara sahip kurallar benimsemeli.

11. Yetkili Otoriteye Karşı Yargı Yoluna Başvurma Hakkı

Veri sahibi, yetkili otoritenin hakkında verdiği bağlayıcılık kararının uygun olmadığı kanısına varır ise, bu otoriteye karşı yargı yoluna gitme hakkına sahiptir.

12. Tazminat Talebi Hakkı

GDPR'ın ihlali sonucu maddi veya manevi zarar gören veri sahiplerinin, bu zarara yol açan kontrolör veya işlemciden, uğradığı zarar için tazminat isteme hakkını da beraberinde getirdiğini söylemek gerekiyor.[6]

[5] http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html

[6] AP ve Avrupa Konseyi," General Data Protection Regulation", 27 Nisan 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf Erişim Tarihi: Ocak 2018

GDPR ve Tüketici Haklarına Etkisi

GDPR'ın tüketiciler için önemli haklar getirdiğini artık biliyoruz. Bu getirdiği hakları bir cümlede özetleyecek olursak GDPR, paylaşmaya karar vermediği sürece, kişisel bilgilerin sadece veri sahibine ait olduğunun altını çiziyor. Tüm kurumlar müşterilerden bilgi toplarken öncelikle izin almak zorunda ve herhangi bir ihlal durumunda tüketicilerin bu duruma el koyma hakları da tüzükle birlikte gelen haklardan.

Hayatımızın her noktasında teknolojiyle iç içe olduğumuz düşünüldüğünde, dijitalleşmenin artılarıyla birlikte olumsuz yönlerinin gün yüzüne çıkması da kaçınılmaz. Herhangi bir siteden günlük hayatta ulaşılması güç kaynaklara erişim, sisteminönemli kazanımı kabul edilirken; *Google* gibi çevrimiçi davranışları izleyen sitelerin bu kaynaklar ile kişiselleştirilmiş pazarlama teknikleri uygulaması, bilgilerimizin hiç de gizli olmadığını ortaya seriyor.

Durum bunlarla da sınırlı değil. Yakın zamanlarda Uber, Equifax gibi uluslararası şirketlerin müşterilerinin ifşalarına neden olması, çalınmış kişisel verilerin karanlık internette satışa çıkarılması, Rusya'nın sızıntılar yoluyla ABD başkanlık seçimlerine müdahele ettiği yönünde spekülasyonlar, teknolojinin karanlık yüzlerinden yalnızca küçük bir kısmı. AB ülkelerinin de benzer durumlardan dolaylı veya dolaysız olarak etkilenmesi kaçınılmaz. GPDR bir bakıma, bu durumlarda AB'nin güvenlik ihtiyacını karşılamak için medet umduğu öncelikli bir araç. Bu tüzük sayesinde tüketiciler servet niteliğindeki verilerini kendi koruma altına alabiliyor. Böylece bankaların, kamu kurumlarının, sigorta şirketlerinin, medikal kurumların, telefon şirketlerinin ve diğer hizmet tedarikçilerinin tüketicinin kişisel bilgilerini gizlilik içerisinde korunması bir zorunluluk haline geliyor. Ayrıca hizmet tedarikçilerinin, edindiği ve işlemek üzere olduğu veri ile ne yapacağı konusunda tüketiciyi bildirmesi sorumluluğu da GDPR sayesinde gerçekleşiyor.

Her ne kadar veri koruma yeni bir olay olmasa da, özellikle küçük çaplı şirketler bu duruma hazır değil, zira çoğu küçük çaplı işletmeler verilerin nerede depolandığı veya transfer edildiğini kayıt altında tutabilmek için gerekli mekanizmaya sahip değil, ayrıca bu mevzuatın kendilerinin de kapsadığından haberleri yok. Bunun yanı sıra Symantex'in iş dünyasının GDPR'a uyum sağlayıp sağlamadığını ölmek amacıyla "Are you compliance-ready?" adlı yaptığı ankete de bakılacak olunursa, büyük çaplı şirketlerin çoğu aynı şekilde bu duruma pek hâkim değil. Bu ankete göre organizasyonların neredeyse tamamı GDPR'ı tam anlamıyla anlamamakla birlikte, uygulamakta başarılı olup olamayacağından emin değil. Ayrıca bu organizasyonların yüzde 26'si 2016 yılında tüzüğün uygulanmasını süre sonuna kadar yetiştirebileceğine inanırken, sadece yüzde 22'si GDPR'ı bir öncelik olarak görüyordu.[7] *Internationl Association of Privacy*

[7] Symantec, "GDPR: Are you compliance ready?", 2017, https://www.symantec.com/content/dam/symantec/docs/infographics/gdpr-are-you-compliance-ready-en.pdf Erişim Tarihi: Ocak 2018

Professionals (IAPP) tarafından AB ve ABD merkezli 500 veri güvenliği uzmanıyla gerçekleştirilen anket çalışması da benzer sonuçları taşıyor. IAPP çalışmasına göre her dört AB merkezli şirketten birinin (yüzde 28) Mayıs 2018'de GDPR'a hazır olması beklenmiyor.[8]

Bir diğer sorun da şu ki, GDPR'ın ana süjeleri tüketiciler bile çoğunlukla bu mevzuatla gelen haklardan haberdar değil. Tüzüğün tam anlamıyla yürürlüğe girmesine aylar kala, tüketicilerin birlikte çalıştıkları kurumlardan güvenlik ilkelerinin değişeceği yönünde e-postalar almaya başlamaları, sürecin yavaş yavaş ciddi bir noktaya geldiğini gösteriyor. Pega adlı müşteri katılımı ve operasyon mükemmelliği doğrultusunda yazılım oluşturan bir kuruluş tarafından tüketicilerin GDPR bilgisini ölçmek amacıyla yapılan anket bu durumu doğrular nitelikte. Yapılan araştırmaya göre, 7 AB ülkesinde 7000'den fazla tüketici GDPR'ın getirdiği hakların neler olduğundan haberdar değil, bu da tüketicilerin yüzde 21'ine tekabül ediyor. Eurobarometre tarafından yapılan araştırmalar da aynı şekilde mevzuattan haberi olmayan çok sayıda AB vatandaşı olduğunu göstermişti. İki araştırmada da ortak görülebilecek bir diğer nokta ise, tüketiciler mevzuattan haberleri olmasa da verilerine tam anlamıyla hâkim olmak istiyorlar. Bu araştırmaya göre, Avrupalı tüketicilerden yüzde 82'si GDPR ile gelen haklarını kullanmaya niyetli olduğunu belirtiyor.[9]

Nihayetinde AB merkezli ve AB ülkeleriyle veri paylaşım etkileşiminde bulunması öngörülen kamu kurumları, veri işleyici özel işletmeler ve veri odaklı sivil toplum kuruluşlarıyla tüketicilerin GDPR konusunda daha ileri seviye farkındalığa ve bilgi birikimine sahip olması gerektiği açık. Önümüzdeki dönemde Türkiye'de de benzer sebeplerden ötürü konunun daha sık şekilde gündeme taşınması gerekiyor. Dolayısıyla AB'nin GDPR çeperinde şekillenmekte olan veri güvenliği ekosisteminin Türkiye'ye halihazırdaki ve öngörülen etkilerini derinlemesine ele almadan önce, AB veri güvenliği ekosisteminde, Türkiye'yi de etkilemesi muhtemel diğer güncel gelişmelere kısaca bakmakta fayda var.

---

[8] IAPP ve TrustArc, Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation,s.9, https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf Erişim Tarihi: Ocak 2018

[9] Eraser, "Know Your Consumer Rights Under The European Union Gdpr", 8 Ağustos 2017, https://eraser.heidi.ie/know-your-consumer-rights-under-the-european-union-gdpr/ Erişim Tarihi: Ocak 2018

AB Veri Güvenliği Ekosistemindeki Güncel Tartışmalar

Güncel sınamalarıyla birlikte AB yönetişim modeli pek çok hızlı gelişmeye karşı hantallıkla ve tepkisizlikle eleştirilse de konu dijital dönüşüm ve veri güvenliği olduğunda, hızlı bir tepkisellikten ve radikal reformist tutumdan bahsetmek mümkün. Bu sebeple de veri güvenliği gündemi çoğu zaman pek çok aktörü içerisine alan tartışmalı gündem maddelerine sahne oluyor. Tartışmalar genellikle GDPR'ın yanında oluşturulması muhtemel ikincil mevzuata ilişkinken, üçüncü ülkelerle veri paylaşımı ve ABAD, AİHM gibi yargı mecralarına taşınan veri güvenliği temalı davalar da gündemi hareketlendiriyor. Bu tartışmalardan, Türkiye'ye de bir şekilde etkisi olacaklara değinmek gerekir.

Veri Koruma Takımının Yeni Üyesi: ePrivacy Tüzüğü

Dijital Tek Pazar Stratejisi'nin temel hedefinin dijital hizmetlerin güvenliğini artırarak, insanların güvenlerini kazanmak olduğunu düşünüldüğünde, GDPR her ne kadar büyük yenilikler getirmiş olsa da, kişisel ve tüzel kişilerin haberleşme gizliliğini ePrivacy Yönergesi koruma altına alıyor. Ancak, ePrivacy Yönergesi de dönemin şartlarına ayak uydurmakta yeterli kalmadığından, bazı revizyonlara ihtiyaç duyuyordu. Bunu, 2016 yılında gerçekleştirilen Eurobarometre anket sonuçlarından da görebiliyoruz. Bu yüzden de daha kapsamlı ve bağlayıcı içeriğe sahip bir ePrivacy Tüzüğü taslağı, Komisyon tarafından hazırlandı ve GDPR ile aynı günde, 28 Mayıs 2018'de yürürlüğe girmesi bekleniyor.

İlk olarak bu tüzük, elektronik haberleşme verilerinin mahremiyetini zorunlu kılıyor; böylece verilerin dinlenmesi, telefon dinlemeleri, görüşmelerin kaydedilmesi, gözetlenmesi, taranması, herhangi bir yolla ele geçirilmesi, elektronik haberleşme verilerinin işlenmesi gibi fiillerin, veri sahibi haricinde kişiler tarafından gerçekleştirilmesini yasaklıyor. [10]

Aynı zamanda ePrivacy Tüzüğü, elektronik iletişim ağ ve hizmet sağlayıcılarını da kısıtlıyor. Bu nedenle elektronik iletişim ağ ve hizmetleri sağlayıcıları, elektronik haberleşme verilerini, iletişimin gerçekleşmesi gerekliliği varsa sadece bu amaç için gerekli süre boyunca işleyebilir. Bahsi geçen durumlara örnek olarak faturalama, ödeme yapma, elektronik iletişim hizmetlerine abonelik gösterilebilir. Tüm bunların yapılabilmesi için ağ ve hizmet sağlayıcıların, veri sahiplerinden izin alması zorunludur.

Kullanıcının rızası da en önemli faktörlerden biri. Kullanıcı bilgilerini depolayabilmek ePrivacy Tüzüğüyle birlikte ancak kullanıcının rızasıyla gerçekleşebilir. Rıza, yazılımların uygun teknik ayarlarını kullanarak ifade edilebilir. Ancak, izni veren veri

[10] Avrupa Komisyonu, "Regulation on Privacy and Electronic Communications", 10 Ocak 2017, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241 Erişim Tarihi: Ocak 2018

sahibi istediği zaman bu rızayı geri çekme hakkına da sahiptir. Ayrıca, elektronik haberleşme sağlayıcıları, veri sahibinden aldıkları içerikleri silmeli veya isimsizleştirmelidir.

Kullanıcıların terminal ekipmanında üçüncü şahısların depolama yapmasının önlenmesi de Tüzüğün önemli özelliklerinden. Yükleme sırasında yazılımlar, kullanıcıları gizlilik ayarları seçenekleri hakkında uyarmalı ve böylece yüklemenin devam edebilmesi için kullanıcının izin vermesi şart koşulmalıdır. Bu madde özellikle önemli, zira ePrivacy Yönergesi'ne göre sitelerin kullanıcılardan bilgi depolayabilmeleri için onlardan izin almaları ancak ekranda çıkan arayüzler sayesinde gerçekleştiriliyor. Bu arayüzler genelde kullanıcıya çerezleri kabul edip etmediğini soran butonlardan oluşuyor, böylelikle de sitenin sahibi için pek kolay yürüyen bir sistem meydana gelmiyor. Tüzükle beraber, site sahipleri kullanıcılara çerezleri kabul edip etmediklerini sormak zorunda kalmayacak zira kullanıcının çerezleri kabul edip etmeyeceği, kullanıcının tarayıcılarında yaptıkları ayarlara bağlı olacak. Her ne kadar site sahiplerinin işi kolaylaşacak gibi görünse de; tarayıcının varsayılan ayarlarının çerezleri kabul etmemek olduğu düşünülürse, bannerlarla bunun belirtilmesi kaçınılmaz. Dolayısıyla, tüzüğün hala geliştirilmesi gerektiği görüşü gün yüzüne çıkıyor.

Yürürlüğe girmesi beklenen ePrivacy Tüzüğü, istenmeyen epostaları, kısa mesajları ve otomatik telefon aramalarını da engelliyor. Kullanıcılar, ya varsayılan olarak ya da pazarlama telefon aramalarını almamak için kara liste oluşturarak koruma altına alınacaklar. Pazarlama yapan şirketler arama yaparken telefon numaralarını gösterme ya da pazarlama amaçlı bir arama olduğunu belirten özel alan kodu kullanma zorunluluğu taşıyacak.

Sonuç olarak, kişisel verilerin neredeyse servet değerinde olduğu ve bundan dolayı büyük kimlik ifşalarının yaşandığı düşünülürse, AB'de pek çok çevrenin veri güvenliğine verdiği önem anlaşılabilir. AB kurumları bu meseleyi daha özel şekilde insan hakları çerçevesinde değerlendirdiğinden, ePrivacy Tüzüğü'nü de içine alan kapsamlı bir mevzuat iyileştirme adımı kaçınılmazdı. Bu yeni tüzükler kamuoyundan bazı eleştiriler almış olsalar da, sürecin nasıl ilerleyeceğini önümüzdeki aylarda göreceğiz.

Brexit Müzakerelerinin Gölgesinde AB'den Üçüncü Ülkelere Veri Paylaşımı

Birleşik Krallık, AB Antlaşması'nın meşhur 50'nci Maddesi'ni 29 Mart 2017 tarihinde devreye sokarak, iki yıl sürmesi öngörülen geçiş aşamasının ardından AB'den ayrılmayı taahhüt etmişti. Bu çerçevede, başka bir karşılıklı ilişki biçimi düzenlenmediği takdirde, 30 Mart 2019 tarihinden itibaren bütün AB müktesebatının geçerliliği, Birleşik Krallık için sona erecek. Buna, AB'nin veri güvenliği mevzuatı da dahil.

Birleşik Krallık'ın GDPR ile AB veri güvenliği ekosisteminin diğer öğelerine uyumu ve bu yapının hangi ölçüde ve hangi statüde parçası olacağı, yukarıda özetlenen durumsalla bağlantılı şekildi büyük merak konusuydu. Komisyonun Adalet ve Tüketiciden Sorumlu

Genel Müdürlüğü, 9 Ocak 2018 tarihinde tüm paydaşlara yönelik bir bilgilendirmede bulunarak konunun bazı boyutlarına açıklık getirdi.

Komisyonun bilgilendirme metninde, Birleşik Krallık'ın AB'den ayrılmasının ardından artık üçüncü ülke statüsüne geçeceği dolayısıyla karşılıklı veri paylaşımına ilişkin süreçlerde AB'nin üçüncü ülkelerle veri paylaşım kurallarının uygulanacağı belirtildi. AB ile yoğun ekonomik ve siyasi etkileşim içerisindeki bir üçüncü ülke olarak Türkiye için de bu değerlendirmeler önem taşıyor.

Güncel konjonktürde AB'nin üçüncü ülkelerle karşılıklı veri paylaşımında bulunabilmesi için üçüncü ülkedeki veri güvenliği standartlarının yeterli seviyeye ulaşmış olması; özel durumların mevcudiyeti veya geçerli önlemleri içeren ikili anlaşmalar aranıyor. GDPR'ın devreye girmesiyle, üçüncü ülkelerin AB ülkeleriyle tematik veri paylaşımını sağlayacak araçların tesisi daha hafifletilmiş bürokratik süreçlerle mümkün olabilecek. Bu boyut, Türkiye açısından da önemli, çünkü her şartta Türkiye'deki hem ulusal mevzuatın hem de mikro ölçekte kurumların iç düzenlemelerinin AB standartlarını sağlaması kritik. AB'nin üçüncü ülkelerle GDPR kapsamındaki veri paylaşımı, önümüzdeki dönemlerde, öne sürdüğü yeni mekanizmalar ve imkanlar çerçevesinde detaylıca ele alınması gereken bir konu. Nitekim halihazırda uygulamada olan karşılıklı veri paylaşım mekanizmalarına ve anlaşmalarına da göz atmak lazım.

AB en güncel bilgiler ışığında Andora, İsviçre, İsrail, Man Adaları, Arjantin, Faroe Adaları gibi birbirinden farklı nitelik ve ölçekteki ülkelerin veri güvenliği standartlarını yeterli kabul etmiş durumda. Japonya ve Güney Kore ile ise müzakereler devam ediyor. Stratejik olarak, AB tarafından büyük ölçekli ticaret müzakerelerinde, hak temelli boyutuyla veri güvenliği meselesi de sıkça gündeme taşınıyor. Dolayısıyla Türkiye ile Gümrük Birliği'nin modernizasyonu sürecinde, konunun gün yüzüne çıkması şaşırtıcı olmayacaktır.[11]

Yukarıdaki bilgiler ışığında, AB'nin tesis ettiği en tartışmalı veri paylaşımı anlaşması şüphesiz ki ABD ile düzenlemiş olduğu Gizlilik Kalkanı (*Privacy Shield*). Hazırlık sürecinde TTIP müzakereleriyle birlikte İKV'nin de çeşitli kereler gündemine aldığı Gizlilik Kalkanı, uluslararası sistemin iki devasa aktörünü biraraya getiren yapısıyla özel vurguyu hak ediyor.

Gizlilik Kalkanı ve Transatlantiğin İki Yakasından Notlar

ABAD'ın meşhur Schrems kararıyla birlikte AB ile ABD arasındaki veri paylaşım serbestliğini garanti altına alan Güvenli Liman (*Safe Harbor*) mekanizmasının askıya alınmasının ardından, temel hak ve özgürlükleri daha ileri seviyede koruması öngörülen

[11] Avrupa Komisyonu, Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en Erişim Tarihi: Ocak 2018

Gizlilik Kalkanı, temmuz 2016'da yetersizliğine ilişkin çok sayıda eleştiriye rağmen yürürlüğe girmişti.

Geçen bir senenin ardından, AB'nin özel veri güvenliği danışma birimi, 29'uncu Madde Çalışma Grubu Kasım 2017 tarihinde, Gizlilik Kalkanı'nı değerlendiren senelik raporunu yayımladı. Genel olarak, tarafların çabaları olumlu karşılanırken, özellikle mekanizmanın bilinirliği, ABD iç hukukuna yansımalarındaki eksiklikler ve ABD'deki denetim/yürütme aygıtlarının güçlendirilmesi gerekliliği vurgulandı. Dolayısıyla bağımsız bir ombudsmanın ve halihazıdaki sorunlu meselelerin çözümüne yönelik bir eylem planının oluşturulması, sıkça gündeme getiriliyor.

Gizlilik Kalkanı'nın kapsadığı iki spesikif alana ilişkin 29'uncu Madde Çalışma Grubu'nun vurgusu önem taşıyor. Çalışma Grubu raporunda, ilk olarak, şirketlerin insan kaynakları birimlerinin, taşımakta oldukları personel bilgilerine dair daha ileri seviye koruma standartlarının sağlanması ikinci olarak ise ABD karar alıcılarının gözetleme, istihbarat faaliyetleri kapsamındaki veri işleme faaliyetlerinde şeffaf olması gerektiği vurgulanıyor.

AB Veri Güvenliği Gündeminin Türkiye'ye Yansımaları

Türkiye'de anayasal bir hak olan kişisel verilerin korunması konusu, uzun yıllar boyunca buz dolabından çıkarılmayı bekleyen mevzuat iyileştirme hamlelerinden biriyken; son 2-3 yılda, Türkiye-AB Vize Serbestliği Diyaloğunun en öncelikli konularından olması sebebiyle beklenmedik derecede hızlı şekilde gündeme taşındı. 2015 yılından bu yana Türk yetkili makamların, tasarı halindeki Kişisel Verilerin Korunması Kanunu üzerinde harcadığı yoğun mesai, ilgili Avrupa Konseyi düzenlemelerinin yüklenilmesi yönünde atılan adımlar ve ulusal çapta bilgilendirme hamleleri; hem Türkiye'nin vizesiz Avrupa ülküsü için değerli hem de dijitalleşen küresel sistemin dinamiklerine ayak uydurabilmek için şarttı.

Yıllarca tasarı olarak TBMM'de bekleyen 6689 sayılı Kişisel Verilerin Korunması Kanunu, teknolojinin gelişmesi, kişisel verilerin önemli varlıklar haline gelmesi ve özellikle Avrupa'da bu konuda çalışmalar yapılması gibi nedenler sonucunda 7 Nisan 2016'da yürürlüğe girdi. GDPR gibi Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi için 2 yıl uyum süresi tanındı ve herhangi bir uzatma öngörülmemesi halinde Nisan 2018'de uygulanmaya başlanacak.

Tasarı halindeki Kanunun yürürlüğe girmesinin ardından Türkiye'de konuya ilişkin teknik ve idari denetimi sağlamakla görevlendirilen Kişisel Verileri Koruma Kurumu[12] vek merkezinde, başkanla birlikte dokuz üyeden oluşan Kişisel Verileri Koruma Kurulu çalışmalarına başladı. Kurumun ilk faaliyetleri, daha çok iç yapının güçlendirilmesi, veri güvenliği kültürünün yaygınlaştırılması ve ilgili kanunun tanıtılmasına yönelik

[12] Kişisel Verileri Koruma Kurumu, http://www.kvkk.gov.tr/

çalışmalar gerçekleştirilmesi ve Kişisel Verilerin Korunması Kanunu'nu tamamlayıcı ikincil mevzuatın meydana getirilmesine yönelikti.

Kanunun yayınlanmasıyla sırasıyla 28 Ekim 2017'de Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkında Yönetmelik, 16 Kasım 2017'de Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına dair Yönetmelik ve 28 Ekim 2017'de Veri Sorumluları Sicili hakkında Yönetmelik, Resmi Gazete'de yayınlandı ve 1 Ocak 2018'de yürürlüğe girdi.

Godot'u bekleyişi andıran uzun hazırlık sürecinin ardından kabul edilen Kişisel Verilerin Korunması Kanunu ve oluşturulan kurul, her ne kadar Türkiye'nin vizesiz AB serüveni için önemli bir adım olarak kabul edilse ve ileri seviye veri güvenliği kültürüne sahip AB ülkelerine Türkiye'yi yakınlaştırmış olsa da bir takım eksikler ilk günden bu yana dile getiriliyor. Özellikle Kişisel Verileri Koruma Kurulu'nun yapısı ve Kanun'daki istisnai hallere ilişkin eleştiriler, hem Türkiye hem de AB'de konuyu yakından takip eden çevrelerce sıkça dile gitirliyor. Dolayısıyla, Türkiye'nin AB ile ileri seviye etkin veri paylaşım işbirliği sağlayabilmesi ve Türkiye'deki kamu, iş dünyası, sivil toplum çevrelerinin GDPR devreye girdikten sonra da etkili şekilde AB'deki paydaşlarıyla dijital işbirliklerini sürdürebilmeleri için Türk mevzuatında iyileştirme şart. Bu iyileştirme özellikle iki alan için fazlasıyla kritik.

Türkiye ve AB Merkezli Kolluk Birimlerinin Karşılıklı Veri İşbirliği

Türkiye-AB ilişkilerine dair son dönemdeki güncel tartışmalarda, retorik sertleşse ve gündem her zamankinden çalkantılı hale gelse dahi ortak tehditlere karşı işbirliği ve terörle mücadele konuları her zaman ortak ajandanın üst sıralarında yer alıyor. Nitekim özellikle Türk tarafında, AB'deki paydaşlarından güvenlik ve istihbarat alanında yeterli desteğin sağlanmadığına ilişkin eleştiriler dikkat çekiyor.

Katılım müzakerelerinin içişleri mevzuatını uyumlaştırmaya yönelik 24'üncü faslına ilişkin ilerleme raporlarındaki değerlendirmeler bu konuya her seferinde yer verirken, AB'nin Türk tarafının eleştirilerine dair tek ve basit bir yorumu var: "Veri güvenliği mevzuatınızı iyileştirin." Önceki bölümlerde bahsedildiği üzere, AB'den üçüncü ülkelerle düzenli, etkin veri akışının sağlanması için o üçüncü ülkedeki veri güvenliği mevzuatının yeterliliği şart. Hele de konu güvenlik ve doğrudan kişilere dair hassas bilgiler olduğunda mevzuat çok daha sert ve eleştirel gözle ele alınıyor.

Halihazırda, Türkiye'nin AB'nin öncelikli kolluk birimleri Europol ve Eurojust ile operasyonel işbirliği bir yandan vize serbestliği diyaloğu çerçevesinde elzem iken, diğer yandan terörle mücadelede işbirliği açısından da kritik. Bu işbirliği de AB kurumlarının Kişisel Verilerin Korunması Kanunu'na yöneltilen eleştirilerinin Türkiye tarafından dikkate alınması ve gerekli iyileştirmelerin sağlanmasıyla mümkün olabilecek. Türk yetkili makamların, vize serbestliği diyaloğunun hızlandırılması için Komisyona iletmeye

hazırlandığı pozisyon belgesinde, bu alanda öngörülen reform hamlelerinin doğru belirlendiğini öngörüyor ve umuyoruz.

AB Veri Güvenliği Gündeminin Türk İş Dünyasına Olası Etkileri

AB ve küresel sistemin demokratik, refah odaklı diğer aktörlerinin dijitalleşme hamlelerine Türkiye'nin de ayak uydurabilmesi için şüphesiz ki kamu sektörüne büyük iş düşse de Türk iş dünyasının sırtındaki yük de ağır sayılır.

25 Mayıs'ta yürürlüğe girecek olan GDPR, AB iş dünyasına, özellikle de şirketlerde belirlenecek olan veri güvenliği sorumlularının (*data protection officer*) sırtına büyük yük eklerken, üçüncü ülkelerdeki paydaşlarıyla veri paylaşımını hızlandırıcı ve kolaylaştırıcı yöntemleri içeriyor. Bunun ise tek şartı var, AB firmalarının üçüncü ülkelerdeki paydaşlarının da etkin veri güvenliği mekanizmalarına ve GDPR'da öne sürülen standartlara sahip olmaları. AB'deki şirketlerin dörtte biri kadarının 25 Mayıs'a kadar hazır olamayacağı dikkate alındığında, bu oranın Türkiye'yi de kapsayan üçüncü ülkelerde çok daha yüksek olması muhtemel.

Türkiye'nin özellikle sanayide küresel düzlemde rekabet edebilir konuma gelmesi, Sanayi 4.0 fenomeninin hızla tüm önkabulleri yıktığı bir dönemde, dijitalleşme rüzgarını yakalamasıyla mümkün. TÜSİAD tarafından *Boston Consulting Group* işbirliğiyle hazırlanan Türkiye'nin Sanayide Dijital Dönüşüm Yetkinliği başlıklı rapor, 2017 yılında Türkiye'deki şirketlerin yüzde 95'inin dijital dönüşüm konusuna ilgi gösterdiğini ortaya koyuyor. Öte yandan aynı rapor, şirketlerin sadece yüzde 61'inin bu dönüşüme hazır olduğunun altını çiziyor. Konu veri güvenliği olduğunda ise karne daha zayıf. Türk iş dünyası tarafından ileri veri güvenliği standartlarının yakalanması gerekliliği henüz bir öncelik dahi kabul edilmiyor. Bu durum TÜSİAD raporunda çok açık ortaya koyulmuş. Dijital dönüşüm yarışını Türkiye'nin önünde sürdüren ülkelerde veri güvenliği eksikliği, dijitalleşme önündeki temel engellerden sayılırken, bu fenomen Türk şirketler için dijitalleşme önündeki ilk 5 tehdit arasında yer almıyor. Bu, bir bakıma Türkiye'de henüz iş dünyasının geneline yayıldığında, veri güvenliği konusuna yeterli önemin verilmediği, farkındalığın sağlanmadığını gösteriyor. Dolayısıyla şirketlerin konuya ilişkin farkındalığının artırılmasında meslek kuruluşlarına, odalar ve borsalarla birlikte teknoloji odaklı sivil toplum kuruluşlarına önemli rol düşüyor.[13]

GDPR ile birlikte yeni bir fırsat penceresiyle karşı karşıya kalması muhtemel olan KOBİ'lere ayrı bir parantez açmak gerekir. Türkiye'nin Sanayide Dijital Dönüşüm Yetkinliği raporu, KOBİ'lerde orta-ileri teknoloji düzeyinde üretim oranını yüzde 24 olarak belirliyor. Bu oran, Türk KOBİ'lerin uluslararası alandaki muadilleriyle rekabetini

[13] Nurşen Numanoğlu ve Hazal İnce, Türkiye'nin Sanayide Dijital Dönüşüm Yetkinliği, TÜSİAD Yayın No. T/2017,12 – 589, Aralık 2017.

büyük ölçüde sınırlarken, veri güvenliği standartları açısından bakıldığında bir fırsat penceresi de sunuyor. Çünkü GDPR, teknoloji yoğun olmayan küçük ve orta ölçekli şirketlere bu anlamda kolaylaştırmalar sağlıyor (veri güvenliği sorumlusu istihdamını zorunlu kılmamak gibi).[14] Dolayısıyla Türk şirketlerin içeride dijital dönüşüm kapasitelerini ve özelde veri güvenliği yeterliliklerini artırmaları lazım. Dışarıya dönük olarak ise tüm paydaşların fırsatlardan haberdar olması şart.

[14] Avrupa Komisyonu, Who does the data protection law apply to, https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en Erişim Tarihi: Ocak 2018