



# Bilgi Güvenliđi ile İlgili Hukuki Mevzuat ve Mevcut Durum

**Av. Emine Devres**

**([emine@devres.net](mailto:emine@devres.net))**

**Devres Hukuk Bürosu**

**İstanbul, Türkiye**



***Mersin Ticaret ve Sanayi Odası***

**Mersin, 29 Mart 2018**



2

# Mevzuat

Ülkemizde bilişim ve bu kapsamda bilgi güvenliği değerlendirildiğinde, Türkiye Cumhuriyeti Anayasası'nın ana çerçeveyi belirlediği görülmektedir.

Anayasa'nın 20. Maddesi gereğince:

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”



3

# Mevzuat

Bilişim alanında işlenen suçlar açısından,

- ❖ 5237 sayılı “Türk Ceza Kanunu”,
- ❖ 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”,
- ❖ 5070 sayılı “Elektronik İmza Kanunu”nu öne çıkar.

Türkiye Avrupa Konseyi 47 ülke tarafından imzalanan “Siber Suçlar Sözleşmesi”ni imzalamıştır.

Anayasa’nın ilgili maddesinin son fıkrasında: Kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alındığından 6698 sayılı “Kişisel Verilerin Korunması Kanunu” yasalaşmıştır.

Tüm bu düzenlemelerin bugün burada konuşulan konulara ve uygulamada karşılaşılan sorunlara tam olarak cevap verebildiğini söylemek maalesef mümkün değildir.



4

# Bilgi Güvenliđi

Bilgi güvenliđinden bahsedebilmek için olmazsa olmaz üç şartın bir arada olması gerekmektedir.

- ❖ Gizlilik (“Confidentiality”)
- ❖ Güvenilirlik (“Integrity”)
- ❖ Hazır Bulunurluk (“Availability”)



5

# Bilgi Güvenliđi

Bugün, bilginin güvenliđini,

- ❖ Belgeleyen
- ❖ İzleyen
- ❖ Belirleyen
- ❖ Devamlılıđını sađlayan
- ❖ Geliřtiren

Uluslararası kuruluş ve organizasyon mevcuttur.

- ❖ ISMS – “Information Security Management System” (Bilgi Güvenliđi Yönetimi)
- ❖ ISO – “International Organization for Standardization” (Uluslararası Standartlar Teřkilatı)



# Bilgi Güvenliğinin Belgelenmesi

6

- ❖ ISO/IEC 27001 – Sistemle Bilgi Güvenliği (“Information Security with a System”)

Küresel virüs saldırılarından endüstriyel casusluğa kadar değişen güvenlik olayları, insanları kontrol edilebilir ve belgelendirilebilir bir bilgi güvenliği yönetim sisteminin gerekliliğine ikna etti.

- ❖ ISO/IEC 27018 – Bulutta Veri Koruması (“Data Protection in the Cloud”)

“Bulutta Veri Koruması”na ilişkin uluslararası standart, mümkün olan en üst seviyede, işlenmiş bilgiyi, ihlallere karşı korumayı amaçlamaktadır.

**Not: IEC (“International Electrotechnical Commission”)**



# Bilgi Güvenliđi

Bilgi güvenliđinin bilincinde olan iř sahipleri ve yneticiler sıklıkla, bilgi güvenliđinin “belgelenebiliyor” olmasına da nem vermekte ve bu belgeleri temin etmeye alıřmakta veya bu belgelere sahip kiři ve/veya kuruluřlar ile alıřmayı tercih etmektedirler.

Gnmzde kiři, kurum ve kuruluřlara ait bilgi varlıklarının hacminin ve eřitliliđinin gemiře oranla ciddi artıřlar gsterdiđi bir vakıadır.

Artık bilgi varlıklarımız ok byk lde sayısallařmıřtır. Bu durum gerek kamu gerekse zel iř srelerini kolaylařtırmakta, gemiřte mmkn olmayan yeni servisler mmkn hale gelmektedir.



8

# Bilgi Güvenliđi

Ancak bütn bunların yanı sıra hayatımızın birçok yönnü ve evresini kapsayan siber uzay alt yapısının güvenliđinin sađlanması konusunun ciddi bir problem olduđu da bir vakıadır.

Başta kamu olmak üzere tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzlukların kişisel, sosyal ve ekonomik hayatımızı önemli ölçde etkilediđi bir gerçektir.

Bu durumda bulut bilişim sisteminde saklanan bilgilere güvenli ulaşım nasıl sađlanacak, bu bilgiler adli süreçte nasıl kabul görp deđerlendirilebilecektir?





# Bulut Bilişim

Bulut bilişim kavramı, Türk Standartları Enstitüsü”nce hazırlanan dokümanda “İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitesinin hızlı bir şekilde artırılıp azaltılabildiği kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.” şeklinde tanımlanmaktadır.



10

# Adli Bilişim

Adli bilişim alanı her geçen gün çok çeşitli problemlerle karşılaşmaktadır. Özellikle muhatap olunan büyük veri, yaygın olarak kullanılan kriptografik uygulamalar, mobil teknolojilerdeki muazzam gelişim ve yasaların teknolojik yeniliklere cevap vermede geç kalması, bunların başlıcaları olarak sıralanabilir.

Bulut bilişim teknolojilerinin hayatımıza iyiden iyiye nüfuz etmeye başladığı günümüzde artık her işlem sadece internete bağlanma uzaklığındadır.



# İhtilaf Çözümü

İş dünyası için bu kadar kolaylık sunan bir sistem ile ilgili bir ihtilaf çıktığında, bu ihtilaf nasıl çözülecektir?

Hukuk sistemimizde asıl olan, iddia sahibin iddiasını ispat etmesidir. İspat vasıtası olan delillerinin de mahkemece kabul gören delillerden olması gerekecektir.

Eğer taraflardan biri, iddiasının ispatı için bulut sistemine kayıtlı bir bilgi ve veriden yararlanmak istediğinde burada dikkat edilmesi gereken husus yukarıda da bahsedilen güvenli bilgi şartlarının karşılanıp karşılanmadığına bakmak gerektiğidir.



12

# Bulut Sisteminin Delil Vasfı

**Kısaca:**

- ❖ Veriyi sisteme aktaran alet ve/veya cihazın,
- ❖ Veriyi sisteme aktaran alet ve/veya cihazın, sistem ile olan iletişiminin,
- ❖ Sistemin kendisinin,
- ❖ Sistemden alınan verinin güvenliği,

**hiçbir şüpheye mahal vermeden ispat edilebiliyor olmalıdır.**

# Bulut Sisteminin Delil Vasfı

- ❖ Başta bahsedilen, veriyi sisteme aktaran alet ve/veya cihaz ile bizzat sistemin kendisinin sahip olduğu ISO/27001 ve ISO/27018 gibi akreditasyon belgeleri ile;
- ❖ Doğrudan sistemden veri alma imkanının sağlanması ile mümkün olabilir.

Şöyle ki:

- ❖ Mahkeme dosyasına ibraz edilecek ISO belgeleri ile veriyi sisteme aktaran alet ve/veya cihazın doğru ölçüm yaptığı, dolayısı ile sisteme aktarılan verilerin gerçek durumu yansıttığı,
- ❖ Yine mahkeme dosyasına ibraz edilecek akreditasyon belgeleri ile veri sisteminin kendisinin güvenliği, ve
- ❖ Mahkemeye verilecek sistem şifreleri ile, mahkeme dosyasına, sistem çıktısı olarak ibraz edilen belgelerin gerçekten de sistemden alındığı ve/veya sistemde yer alan bilgiler ile bire bir aynı olduğu teyid edilebilir.



14

# Bulut Sisteminin Delil Vasfı

Böylece, bulut sisteminde kayıtlı olan bilgi/veya veriye dayanan taraf iddiasını ispat şansına kavuşabilir.

İş dünyası için büyük kolaylık olan bulut sisteminin, böylece ihtilaflarda delil olma vasfı kazanması ile taraflar ileride doğabilecek ihtilaflara karşı, zamanın ruhuna ve temposuna uymayan, delil yaratma çabası içerisinde kalmak zorunda olmazlar.

Hukuk ve yargı sistemimizin teknolojideki ve bulut sistemindeki yenilik ve değişikliklere adapte olarak, sistemin kolaylıklarını kendi bünyesine de alması gerekmektedir. Uygulamacıların günlük hayatta karşılaştıkları zorluklar dikkate alınarak bunlara çözüm üretmek gerekmektedir.



Umarım ve dilerim ki yakın zamanda olumlu gelişmeler görebiliriz.

**Av. Emine Devres**  
([emine@devres.net](mailto:emine@devres.net))  
**Devres Hukuk Bürosu**  
**İstanbul, Türkiye**



8. Tarım, Gıda ve Soğuk Zincir Lojistiği: Soğuk Zincir Lojistiğinde Yenilikçi Çözümler  
Mersin, 29 Mart 2018