

Siber Güvenlik Kanununda Veriye Erişme ile Erişime Açma Ayrımı

Kamuoyunda panel olarak adlandırılan sorgu arayüzlerine ilişkin soruşturmalar, son dönemde geniş bir fail çevresine yayılmıştır.

Av. Burak Üçüncü · 5 Eylül 2026 · 8 dk okuma

Kamuoyunda panel olarak adlandırılan sorgu arayüzlerine ilişkin soruşturmalar, son dönemde geniş bir fail çevresine yayılmıştır. Alacak tahsili yapan işletmelerin operasyon birimleri, gayrimenkul ve sigorta aracılığı faaliyeti yürütenler, insan kaynakları çalışanları, özel güvenlik ve araştırma hizmeti veren şirketler, basın mensupları ve serbest meslek erbabı, birbirinden hayli farklı fiiller sebebiyle aynı soruşturma dosyalarında yer almaktadır. Bu soruşturmalarda sevk maddesi olarak ağırlıklı biçimde 7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin dördüncü fıkrası esas alınmaktadır.

Bu çalışmada, anılan fıkranın maddi ve manevi unsurları incelenmekte, hükmün seçimlik hareketleri ile suçun konusuna ilişkin nitelemenin uygulamada nasıl genişletildiği tartışılmakta ve hükmün uygulanamadığı hâllerde başvurulması gereken normlar belirlenmektedir. İnceleme, [panel davaları](#) bakımından sevk maddesinin doğru tespitine yönelik olup, fiillerin hukuka aykırılığını tartışma konusu yapmamaktadır.

BÖLÜM II

Hükmün Metni ve İnceleme Konusu

Siber Güvenlik Kanunu m. 16/4 uyarınca, siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri, kişilerin veya kurumların izni olmaksızın ücretli veya ücretsiz şekilde erişime açan, paylaşan veya satışa çıkaranlar hakkında üç yıldan beş yıla kadar hapis cezasına hükmolunur.

Panel olarak adlandırılan yapılar, farklı zamanlarda çeşitli kurum ve işletmelerden hukuka aykırı biçimde çıkarılmış veri kümelerinin birleştirilerek tek bir sorgulama arayüzünde sunulmasından ibarettir. Bu yapıların ortaya çıkışında, veri sorumlusu sıfatını haiz kuruluşlardaki güvenlik zafiyetlerinin belirleyici rol oynadığı, buna karşılık söz konusu ihlaller bakımından yürütülen soruşturmaların sınırlı kaldığı gözlenmektedir. Ceza politikasının zincirin kaynağındaki yapısal sorumluluk yerine son kullanıcıya yönelmesi, ayrıca değerlendirilmeyi gerektiren bir tercihtir. Bununla birlikte bu tespit, fiilin hukuka aykırılığını ortadan kaldırmayıp, yalnızca uygulamanın yaygınlık sebebini açıklamaktadır.

Uygulamada karşılaşılan temel sorun, panel niteliğindeki bir arayüz üzerinden sorgulama yapan kişinin fiilinin, hükümde sayılan seçimlik hareketlerden birini gerçekleştirdiği kabulüyle bu fıkra kapsamında

değerlendirilmesidir. Oysa hükmün lafzı ile bu kabul arasında, ceza hukuku bakımından giderilmesi güç bir mesafe bulunmaktadır.

BÖLÜM III —

Suçun Maddi Unsurları

A. Fiil unsuru

Fıkra üç seçimlik hareket öngörülmüştür. Bunlar erişime açma, paylaşma ve satışa çıkarma fiilleridir. Anılan hareketlerin ortak niteliği, verinin failin hâkimiyet alanından çıkarak üçüncü kişilerin bilgisine ya da tasarrufuna sunulmasıdır. Her üç fiil de dışa yönelik bir hareketi tanımlamaktadır.

Buna karşılık erişme, sorgulama, görüntüleme ve indirme fiilleri hükümde sayılmamıştır. Bu husus bir kanun boşluğu olarak değerlendirilemez. Nitekim kanun koyucu aynı maddenin altıncı fıkrasında, siber saldırı neticesinde elde edilen verinin siber uzayda bulundurulmasını ayrıca ve bağımsız biçimde cezalandırmayı tercih etmiştir. Kanun koyucunun aynı madde içinde pasif tasarruf biçimlerini düzenlemeyi bildiği hâlde dördüncü fıkra bu yola gitmemiş olması, söz konusu fıkra yalnızca aktif yayma hareketlerinin suç tipine dâhil edildiği sonucunu doğrulamaktadır.

Bu itibarla panel niteliğindeki bir arayüzden sorgulama yapmak ile paneli veya panelden elde edilen verileri üçüncü kişilerin kullanımına sunmak, aynı suç tipinin farklı görünüşleri değil, birbirinden bağımsız fiillerdir.

B. Suçun konusu

Hükmün çoğu zaman gözden kaçan yönü, suçun konusuna ilişkin nitelemedir. Fıkra, korunan değeri siber uzayda veri sızıntısı nedeniyle daha önce yer alan veriler biçiminde tarif etmektedir. Bu niteleme tek bir koşul değil, birlikte gerçekleşmesi gereken üç ayrı koşul içermektedir.

Öncelikle ortada kişisel veri ya da kritik kamu hizmeti kapsamına giren kurumsal veri niteliğinde bir veri bulunmalıdır. İkinci olarak bu verinin siber uzaydaki mevcudiyeti bir veri sızıntısından kaynaklanmalıdır. Üçüncü olarak söz konusu mevcudiyet, isnat edilen fiilden önceki bir zaman dilimine ait olmalıdır. Bu üç koşuldan biri gerçekleşmediğinde hüküm uygulama alanı bulmaz.

Uygulamada iddianamelerin bu unsurları ayrı ayrı ortaya koymadığı görülmektedir. Verinin hangi ihlal olayından kaynaklandığı, bu olayın tarihi ve ele geçirilen veri kümesiyle ilişkisi çoğunlukla gösterilmemektedir. Bir panelde yer alan verinin kaynağı, kamuya açık kaynaklardan derleme olabileceği gibi, yetkili bir sistemden yetki aşımı suretiyle çıkarılmış ya da doğrudan ilgili kişinin kendi paylaşımlarından toplanmış da olabilir. Bu ihtimallerin hiçbiri veri sızıntısı kavramını kendiliğinden karşılamamaktadır. Panelin mevcudiyeti, sızıntının ispatı yerine geçmez ve ispat yükü iddia makamındadır.

BÖLÜM IV —

Kanunilik İlkesi Bakımından Değerlendirme

Türk Ceza Kanunu'nun 2. maddesinin üçüncü fıkrası, kanunların suç ve ceza içeren hükümlerinin uygulanmasında kıyas yapılamayacağını ve bu hükümlerin kıyasa yol açacak biçimde geniş yorumlanamayacağını düzenlemektedir.

Panel davalarında sıklıkla başvuru alan akıl yürütme, failin sorgulama yapabilmesinin ancak verinin ona açılmış olmasıyla mümkün olduğu, dolayısıyla failin de erişime açma düzeninin bir parçası sayılması gerektiği yönündedir. Bu yaklaşım, bir failin ceza sorumluluğunu başka bir failin fiilinden türetmekte ve ceza sorumluluğunun şahsiliği ilkesiyle bağdaşmamaktadır. Kaldı ki hukuk düzeninde benzer ilişkiler bakımından verilen ile alanın ayrı ayrı düzenlenmesi istisna değil, kural niteliğindedir.

Kanunilik ilkesinin bu bağlamdaki işlevi, failin cezasız kalmasını sağlamak değil, isnadın kanunun öngördüğü fiille örtüşmesini temin etmektir. Toplumsal tepkinin yoğunluğu, suç tipinin sınırlarını genişleten bir yorum ölçütü olarak kullanılamaz. Aksi hâlde belirli bir alanda kabul edilen esnek yorum, sonraki uygulamalarda başka suç tipleri bakımından da emsal teşkil eder ve normun öngörülebilirlik niteliği zedelenir.

Bilişim alanına ilişkin suç tiplerinde bu risk daha da belirgindir. Erişim sağlama, erişime açma ve erişilebilir kılma kavramları gündelik kullanımda birbirinin yerine kullanılmakta, ancak ceza normunda farklı seçimlik hareketleri ifade etmektedir. Kanaatimizce erişime açma kavramının erişmeyi de kapsayacak biçimde yorumlanması, seçimlik hareketin genişletilmesi sonucunu doğurmakta ve kanunilik ilkesinin ihlali anlamına gelmektedir. Siber suç isnadı içeren dosyalarda savunmanın ilk aşamada üzerinde durması gereken husus da bu kavram kaymasıdır.

BÖLÜM V —

Ortak Sisteme Aktarım Hâlinde Erişime Açma Fiilinin Oluşumu

Yukarıdaki değerlendirme, panelden veri temin eden her failin m. 16/4 kapsamı dışında kaldığı anlamına gelmemektedir. Fıkranın gerçekten tartışılabilir hâle geldiği durum, panelden elde edilen verilerin bir işletmenin ortak dosya sistemine, müşteri yönetim yazılımına, çağrı merkezi ekranına, kurum içi veri tabanına ya da çok kullanıcı bir mesajlaşma grubuna aktarılmasıdır. Bu hâlde fail yalnızca veriye erişmemekte, daha önce bu veriye erişim imkânı bulunmayan üçüncü kişilerin erişimini mümkün kılmaktadır. Erişime açma fiilinin oluştuğu sonucuna bu durumda ulaşılabilir.

Ancak bu sonuç da kendiliğinden doğmaz. Ortak sistemde hangi verinin bulunduğu, bu veriye kaç kullanıcının yetkili olduğu, aktarımın kim tarafından ve hangi tarihte gerçekleştirildiği teknik olarak ortaya konulmalıdır. Failin yalnızca kendi cihazında tuttuğu bir kayıt ile çok kullanıcı bir alana yerleştirdiği kayıt arasındaki fark, suç tipinin oluşup oluşmadığını belirlemektedir. Erişim kayıtları, yetkilendirme matrisleri ve paylaşım izleri incelenmeksizin yapılacak nitelendirme varsayıma dayanacaktır.

Aktarımın kapsamı bakımından da derecelendirme yapılması gerekir. Verinin belirli bir dosya kapsamında ve sınırlı sayıda yetkili kişiye ulaştırılması ile kurum genelinde süresiz biçimde erişilebilir kılınması, hem fiilin ağırlığı hem de neticenin kapsamı bakımından aynı değerlendirmeye tabi tutulamaz. Erişime açma fiilinin oluştuğu kabul edilse dahi, bu husus temel cezanın belirlenmesinde gözetilmelidir.

BÖLÜM VI —

Manevi Unsur

Fıkra düzenlenirken suç, ancak kastla işlenebilir. Failin, eriştiği verinin daha önce bir veri sızıntısı sebebiyle siber uzayda yer alan kişisel veri niteliğinde olduğunu bilmesi ve buna rağmen onu üçüncü kişilerin erişimine açmayı istemesi aranır.

Uygulamada bu unsurun ayrıca tartışılmadığı gözlenmektedir. Kendisine adres doğrulama ya da benzeri bir hizmet sunulduğu izlenimiyle hareket eden ve verinin kaynağı hakkında bilgisi bulunmayan kullanıcı ile veri kümesinin niteliğini bilerek ticari faaliyet yürüten kişi, aynı ölçütle değerlendirilmektedir. Kastın ispatı iddia makamına ait olup, panelin mevcudiyeti tek başına failin bilgisini ortaya koymaz. Bu husus, sevk maddesine ilişkin itirazdan bağımsız ikinci bir savunma hattı oluşturmaktadır.

BÖLÜM VII —

Hükmün Uygulanamadığı Hâllerde Başvurulacak Normlar

Yapılan değerlendirme, fiilin hukuka uygun sayılması sonucunu doğurmaz. m. 16/4 unsurları itibarıyla gerçekleşmediğinde, fiil bakımından Türk Ceza Kanunu'nun kişisel verilere ilişkin hükümleri gündeme gelir.

Panel üzerinden sorgulama yaparak veriyi temin eden fail bakımından tipik niteleme, kişisel verileri hukuka aykırı olarak ele geçirmeyi düzenleyen TCK m. 136'dır. Elde edilen verinin faile ait bir sisteme kaydedilmesi hâlinde kişisel verilerin kaydedilmesi suçunu düzenleyen TCK m. 135 uygulama alanı bulur. Erişimin yetkisiz biçimde bir bilişim sistemine girmek suretiyle sağlanması durumunda ise TCK m. 243 ve devamındaki hükümler değerlendirilmelidir.

Ayrıca fiilin, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında veri sorumlusu ya da veri işleyen sıfatıyla gerçekleştirilmesi hâlinde, ceza sorumluluğundan bağımsız olarak idari yaptırım sorumluluğu doğar. Ceza soruşturmasıyla idari sürecin birbirinden bağımsız yürüdüğü ve birinde verilen kararın diğeri bakımından kesin hüküm teşkil etmediği göz önünde bulundurulmalıdır.

Anılan hükümlerin öngördüğü yaptırımlar m. 16/4'e nazaran daha hafiftir. Ancak mesele yaptırımın ağırlığı değil, fiile uyan normun tespitidir. Sevk maddesinin belirlenmesi tutuklama tedbirine başvurulup başvurulamayacağını, adli kontrol tedbirlerinin kapsamını, dava zamanaşımı süresini, uzlaştırma ve hükmün açıklanmasının geri bırakılması kurumlarının uygulanabilirliğini doğrudan etkilemektedir.

BÖLÜM VIII —

Soruşturmanın Kurgusu ve Delil Hukuku

Panel kullanımının tespiti tek başına sevk maddesini temellendirmeye elverişli değildir. Dosyanın usulüne uygun kurulabilmesi için birbirinden bağımsız soruların cevaplanması gerekir. Veriye kimin eriştiği, veriyi kimin erişime açtığı ve erişimin kimlere sağlandığı ayrı ayrı belirlenmelidir. Buna, erişilen bilginin gerçekten korunmaya değer bir kişisel veri mi yoksa hukuken herkesin ulaşabileceği bir bilgi mi olduğu sorusu eklenmelidir.

Bu ayrımlar yapılmaksızın, tek bir ödeme kaydı, tek bir bağlantı izi ya da bir mesajlaşma grubundaki üyelik esas alınarak çok sayıda şüpheli hakkında aynı maddeden işlem tesis edilmektedir. Kolektif nitelemenin ceza sorumluluğunun şahsiliği ilkesiyle bağdaşmadığı açıktır.

Söz konusu dosyalar ağırlıklı olarak dijital delile dayandığından, delilin elde ediliş usulü de nitelemeyi doğrudan etkilemektedir. Arama ve el koyma işleminin kapsamı, cihaz imajının alınıp alınmadığı, özet değerinin usulüne uygun kaydedilip kaydedilmediği, incelemenin yedek üzerinden yürütülüp yürütülmediği ve üçüncü kişilere ait verilerin ayıklanıp ayıklanmadığı ayrıca denetlenmelidir. Bir panelin sunucu kayıtlarında görünen kullanıcı adının şüpheliye aidiyeti dahi başlı başına bir ispat sorunudur. Paylaşılan bağlantılar, devredilmiş hesaplar ve tarih uyumsuzlukları bu dosyalarda sık karşılaşılan durumlardır.

Dijital delilin değerlendirilmesinde gözetilmesi gereken bir diğer husus, panelden yapılan sorgulamanın niceliği ile fiilin niteliği arasında doğrudan bir bağ kurulamayacağıdır. Çok sayıda sorgulama yapılmış olması, tek başına verinin üçüncü kişilerin erişimine açıldığını göstermez; nitekim aynı verinin farklı tarihlerde tekrar sorgulanması da mümkündür. Buna karşılık tek bir sorgulama, elde edilen verinin çok kullanıcı bir alana aktarılması hâlinde fıkra kapsamına girebilir. Bu itibarla nicelik ölçütünün nitelik değerlendirmesinin yerine geçirilmesi hatalıdır.

BÖLÜM IX

Veri Sorumlusu Sıfatı Bakımından Kurumsal Sorumluluk

Panel kullanımı yalnızca bireysel ceza sorumluluğu doğurmamaktadır. Çalışanların sorgulama yaptığı işletmeler bakımından veri sorumlusu sıfatından kaynaklanan idari yaptırım riski, iş hukuku boyutu ve ilgili kişilere karşı tazminat sorumluluğu da gündeme gelir. Bu değerlendirmede belirleyici olan, sorgulamanın çalışanın kişisel inisiyatifiyle mi yoksa fiilen kurumsallaşmış bir çalışma yöntemi olarak mı gerçekleştirildiğidir.

Yazılı veri erişim politikası bulunan, yetkilendirme matrisi tutan, erişim kayıtlarını saklayan ve çalışanlarına yönelik eğitim faaliyetini belgeleyebilen işletmeler, hem idari süreçte hem ceza soruşturmasında daha savunulabilir bir konumda bulunur. Bu altyapının yokluğunda bireysel bir fiilin kurumsal politika olarak nitelendirilmesi ihtimali güçlenir.

İşveren bakımından ayrıca, çalışanın fiilinden doğan sorumluluğun sınırları belirlenmelidir. Sorgulamanın işverenin bilgisi ve talimatı dışında gerçekleştirildiğinin ortaya konulabilmesi, hem ceza soruşturmasında hem de işverene yöneltilecek tazminat taleplerinde belirleyici olacaktır. Bu tespitin yapılabilmesi ise ancak önceden kurulmuş bir kayıt ve yetkilendirme düzeninin varlığı hâlinde mümkündür.

BÖLÜM X

Sonuç

Siber Güvenlik Kanunu m. 16/4, hem seçimlik hareketleri hem de suçun konusunu dar ve katmanlı biçimde düzenlemiştir. Erişme fiili hükümde sayılmamış olup, erişime açma kavramının erişmeyi kapsayacak biçimde yorumlanması kanunilik ilkesine aykırılık teşkil eder. Suçun konusuna ilişkin üç koşulun somut olayda ayrı ayrı ortaya konulamadığı dosyalarda ise hüküm hiç uygulanamaz ve değerlendirme Türk Ceza Kanunu'nun kişisel verilere ilişkin hükümlerine intikal eder.

Ortak sisteme aktarım hâlinde fıkranın uygulanabilirliği ciddi biçimde tartışılabilir olmakla birlikte, bu sonuç da teknik tespit yapılmaksızın kabul edilemez. Panel davaları bakımından soruşturmanın erken aşamasında dijital delilin usulüne uygun elde edilip edilmediğinin ve sevk maddesinin isabetinin denetlenmesi, yargılamanın seyrini belirlemektedir. Bu nedenle sürecin bilişim hukuku alanında çalışan bir vekil eşliğinde yürütülmesi isabetli olacaktır.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/siber-guvenlik-kanununda-veriye-erisme-ile-erisime-acma-ayrimi>