7545 SAYILI SİBER GÜVENLİK KANUNU M.16/4 ANALİZİ

Hazırlayan: Onur Ege Tarhan

Öğrenci No: 125692029

1 Giriş

1.1 İncelenen Hüküm

Bu bölümde 7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin dördüncü fıkrası incelenmektedir. Hüküm özetle, siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel verilerin veya kritik kamu hizmeti kapsamına giren kurumsal verilerin, kişiler ya da kurumların izni olmaksızın ücretli veya ücretsiz biçimde erişime açılması, paylaşılması veya satışa çıkarılması halinde üç yıldan beş yıla kadar hapis cezası öngörmektedir.[1]

Hüküm, 7545 sayılı Kanun'un cezai hükümler ve idari para cezalarına ilişkin 16. maddesi içinde yer almaktadır. Aynı maddede bilgi ve belge vermeme, gerekli izin veya onay olmaksızın faaliyet yürütme, sır saklama yükümlülüğünün ihlali, gerçeğe aykırı veri sızıntısı içerikleri, Türkiye Cumhuriyeti'nin siber uzaydaki milli gücüne yönelik saldırılar ve bazı idari para cezaları da düzenlenmiştir.[2] Türkiye Adalet Akademisi Dergisi'nde yayımlanan bir çalışmada da m.16'nın Türk hukukunda ilk kez bu alanda farklı suç tipleri yarattığı belirtilmektedir.[3]

1.2 Korunan Hukuki Değer

M.16/4 ile korunan hukuki değer birden fazla alanı ilgilendirmektedir. İlk bakışta hüküm kişisel verilerin ve kritik kamu hizmeti kapsamındaki kurumsal verilerin gizliliğini korumaktadır. Ancak hükmün amacı yalnızca bireyin mahremiyetini korumakla sınırlı değildir. Veri sızıntısı sonrasında verilerin yeniden dolaşıma sokulması, siber olayın etkisini büyütür; mağdur kurumun itibarını zedeler; dolandırıcılık, kimlik hırsızlığı ve ikincil saldırılar için zemin oluşturur. Kritik kamu hizmetleri söz konusu olduğunda ise bu risk kamu düzeni ve hizmet sürekliliği boyutuna ulaşabilir.

Bu nedenle hükmün arkasındaki temel düşünce, veri sızıntısını tek bir teknik olay olarak görmemek; sızıntıdan sonra verinin paylaşılması ve ticari meta haline getirilmesiyle oluşan ikincil zararı cezalandırmaktır. Bu yaklaşım yerindedir. Çünkü güncel siber suç ekonomisinde çalınmış veri, yalnızca saldırının sonucu değil, aynı zamanda yeni suçların başlıca nedeni haline gelmiştir.

1.3 Suçun Maddi Unsuru

1.3.1 Suçun Konusu

Suçun konusu iki kategoriden oluşmaktadır. İlk kategori kişisel verilerdir. İkinci kategori ise kritik kamu hizmeti kapsamına giren kurumsal verilerdir. Bu kategori, doğrudan bireye ait olmasa da kamu hizmetlerinin sürekliliği ve güvenliği açısından önem taşıyan kurum verilerini kapsar.

Hükümde özellikle "siber uzayda veri sızıntısı nedeniyle daha önce yer alan" verilerden söz edilmesi önemlidir. Bu ifade, suçun konusunun her türlü veri olmadığını; daha önce bir sızıntı neticesinde siber uzaya düşmüş veri olduğunu göstermektedir. Ancak bu ifade aynı zamanda belirsizlik yaratır. "Daha önce yer alma" ifadesinin yalnızca dark web sızıntı sitelerini mi, herkese

---

[1] 7545 sayılı Siber Güvenlik Kanunu, m.16/4, Resmi Gazete, 19.03.2025, sayı 32846.

[2] 7545 sayılı Siber Güvenlik Kanunu, m.16, Resmi Gazete, 19.03.2025, sayı 32846.

[3] Cem Şenol, "7545 Sayılı Siber Güvenlik Kanunu'nda Düzenlenen Suçlar", Türkiye Adalet Akademisi Dergisi, 2025, sayı 63, https://dergipark.org.tr/tr/pub/taad/article/1751122

açık forumları mı, mesajlaşma kanallarını mı, bulut depolarını mı, yoksa arama motorlarıyla bulunabilen tüm içerikleri mi kapsadığı açık değildir.

1.3.2 Fiil

Hüküm üç seçimlik hareket öngörmektedir: erişime açma, paylaşma ve satışa çıkarma. Ücretli veya ücretsiz olması sonucu değiştirmez. Bu tercih isabetlidir, çünkü sızdırılmış verinin ücretsiz paylaşılması da zarar yaratır. Hatta bazı durumlarda ücretsiz paylaşım, verinin daha hızlı yayılmasına ve geri döndürülemez hale gelmesine neden olabilir.

Buna karşılık fiillerin sınırı iyi çizilmelidir. Örneğin bir gazetecinin veri sızıntısını haberleştirmesi, bir güvenlik araştırmacısının örnek veri göstermeden ihlali raporlaması veya mağdur kişilerin zararı anlaması için sınırlı bilgilendirme yapılması aynı kapsamda değerlendirilmemelidir. Hükümde bu tür meşru faaliyetleri koruyan açık bir istisna bulunmaması, uygulamada ifade özgürlüğü ve kamu yararı tartışmalarına yol açabilir.

1.3.3 Fail ve Mağdur

Suç herkes tarafından işlenebilir. Failin ilk sızıntıyı gerçekleştiren kişi olması gerekmez. Bu yönüyle hüküm, veri sızıntısından sonra veriyi yeniden yayan üçüncü kişileri de hedeflemektedir. Mağdur, somut olaya göre kişisel verisi yayılan gerçek kişi, kurumsal verisi sızdırılan kurum veya kritik hizmetin etkilenmesi nedeniyle toplum olabilir.

Bu geniş fail yapısı yerindedir. Çünkü sızıntı verileri çoğu zaman ilk saldırgan dışında çok sayıda aracı hesap, forum kullanıcısı, veri simsarı veya ikincil dolandırıcı tarafından dolaşıma sokulmaktadır. Yine de failin verinin kaynağını ve hukuka aykırı niteliğini bilip bilmediği, manevi unsur bakımından dikkatle değerlendirilmelidir.

1.4 Manevi Unsur

Hükümde özel kast açıkça düzenlenmemiştir. Bu nedenle suçun kasten işlenebileceği kabul edilmelidir. Failin veriyi erişime açtığını, paylaştığını veya satışa çıkardığını bilmesi ve istemesi gerekir. Ancak failin verinin siber uzayda veri sızıntısı nedeniyle yer aldığını bilip bilmediği uygulamada tartışma yaratabilir.

Kanaatimce bu suçta en kritik nokta, failin verinin sızıntı kaynaklı ve izinsiz olduğunu bilmesi veya en azından bu konuda ciddi bir şüpheye rağmen hareket etmesidir. Aksi halde, örneğin internette zaten herkese açık olduğunu düşündüğü bir veri setini hukuki niteliğini bilmeden aktaran kişi ile sızıntı sitesinden veri indirip satan kişi aynı kefeye konulmuş olur. Ceza hukukunda kusur ilkesi gereği bu ayrımın yapılması gerekir.

1.5 Hukuka Aykırılık ve Olası İstisnalar

Hükümde “kişilerin veya kurumların izni olmaksızın” ifadesi yer almaktadır. Ancak kişisel veriler bakımından yalnızca “izin” kavramı yeterli değildir. Kişisel verilerin işlenmesinde genel ilkeler ve işleme şartları değerlendirilir. Bu nedenle m.16/4’teki izin kavramının KVKK ile uyumlu yorumlanması gerekir.

Ayrıca kamu yararı, haber verme, akademik araştırma, siber olay müdahalesi, zafiyet bildirimi ve yargı ya da idari makam bildirimleri gibi alanlarda özel istisna ihtiyacı vardır. Aksi halde iyi niyetli

güvenlik araştırmacıları veya veri ihlalini sorumlu biçimde raporlayan kişiler bakımından caydırıcı bir etki doğabilir.

1.6 Diğer Suçlarla İlişki

1.6.1 TCK m.136 ile İlişki

TCK m.136, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme fiillerini cezalandırmaktadır. 7545 sayılı Kanun m.16/4 ise siber uzayda veri sızıntısı nedeniyle yer alan kişisel verilerin veya kritik kamu hizmeti kapsamındaki kurumsal verilerin erişime açılması, paylaşılması veya satışa çıkarılmasını düzenlemektedir.

M.16/4'ün özel hüküm olarak uygulanabileceği durumlar bulunabilir. Ancak bu özel hükmün sınırı açık çizilmezse, aynı fiilin hem TCK m.136 hem de 7545 sayılı Kanun m.16/4 kapsamında değerlendirilmesi ve fikri içtima tartışmaları doğabilir. Özellikle yalnızca kişisel veri içeren bir sızıntı dosyasının paylaşılması halinde hangi hükmün öncelikli uygulanacağı uygulamada önem kazanacaktır.

1.6.2 TCK m.243 ve m.244 ile İlişki

M.16/4, sızıntı verisinin paylaşılması aşamasını hedefler. İlk saldırı, sisteme girme veya sistemin işleyişini bozma aşamasında gerçekleşmişse TCK m.243 ve m.244 de gündeme gelebilir. Böyle bir olayda saldırganın eylemleri parçalara ayrılarak değerlendirilmelidir: sisteme yetkisiz giriş, verinin ele geçirilmesi, sistemin şifrelenmesi, verinin yayımlanması tehdidi ve verinin fiilen yayımlanması ayrı hukuki nitelikler taşıyabilir.

1.6.3 KVKK ile İlişki

KVKK, veri sorumlusuna kişisel verilerin güvenliğini sağlama yükümlülüğü yükler. Bir veri ihlali olduğunda veri sorumlusu, ihlali Kişisel Verileri Koruma Kuruluna ve ilgili kişilere bildirmek zorunda kalabilir. M.16/4 ise veri sorumlusunun ihmalinden çok, sızdırılmış veriyi izinsiz dolaşıma sokan kişinin cezai sorumluluğuna odaklanır. Bu nedenle iki düzenleme birbirini tamamlar. Ancak veri sorumlusunun kusuru ile veriyi yayan üçüncü kişinin kastı ayrıştırılmalıdır.

1.7 Yaptırım ve Orantılılık

Hüküm üç yıldan beş yıla kadar hapis cezası öngörmektedir. Bu ceza alt sınırı itibarıyla oldukça ciddidir. Veri sızıntısı sonrası verinin satılması veya geniş kitlelere yayılması ağır bir tehlike yarattığından yaptırımın caydırıcı olması anlaşılabilir. Ancak hüküm, çok farklı ağırlıktaki fiilleri aynı ceza aralığına toplamaktadır. Örneğin yüz binlerce kişinin kimlik verisini dark web pazarında satışa çıkaran kişi ile sınırlı sayıda kurumsal veriyi küçük bir grupta paylaşan kişi aynı ceza aralığına girmektedir.

Bu nedenle hükümde nitelikli hallerin ve daha hafif hallerin açıkça ayrılması daha isabetli olurdu. Özel nitelikli kişisel veriler, çocuklara ait veriler, kimlik belgesi görüntüleri, sağlık verileri, finansal erişim bilgileri, kritik altyapı hizmet sürekliliğini tehlikeye atan veriler ve kazanç amacıyla yapılan satışlar daha ağır yaptırıma bağlanabilir. Buna karşılık kamu yararı amacıyla, veri örneği göstermeden yapılan sorumlu bildirimlerin suç dışında kalması gerekir.

1.8 Hükmün İhdas Edilmesinin Yerindeliği

Kanaatimce bu suç tipinin ihdas edilmesi genel olarak yerindedir. Çünkü modern siber saldırılarda verinin sızdırılması çoğu zaman saldırının sonu değil, ikinci aşamasıdır. Sızıntı verileri forumlarda, dark web pazarlarında ve mesajlaşma kanallarında yeniden dolaşıma sokuldukça zarar büyür. Ayrıca mağdur kişi için zarar yalnızca ilk ihlal anında değil, verinin yıllarca farklı ortamlarda yeniden paylaşılmasıyla devam eder.

Bununla birlikte hükmün mevcut hali bazı yönlerden sorunludur. Birincisi, "siber uzayda veri sızıntısı nedeniyle daha önce yer alan" ifadesi uygulama bakımından belirsizdir. İkincisi, "izin" kavramı kişisel veriler bakımından KVKK sistematiğini tam karşılamamaktadır. Üçüncüsü, yaptırım farklı ağırlıktaki fiilleri yeterince ayırmamaktadır.

Bu nedenle hükmün amacı doğru olmakla birlikte, norm tekniği bakımından daha belirli ve ölçülü hale getirilmesi gerekir.

1.9 Alternatif Hüküm Önerisi

Aşağıdaki metin, m.16/4'ün amacını koruyup belirlilik ve ölçülülük sorunlarını azaltmak için önerilmektedir:

Hukuka aykırı sızıntı verilerinin yayılması ve ticari kullanımı

Madde X -

1. Bir siber olay veya siber saldırı sonucunda hukuka aykırı olarak elde edildiğini bildiği kişisel verileri ya da kritik kamu hizmetinin güvenliğini veya sürekliliğini etkileyebilecek kurumsal verileri, ilgili kişinin, kurumun veya kanunen yetkili merciin hukuka uygun izni bulunmaksızın siber ortamda erişime açan, paylaşan, devreden veya satışa arz eden kişi iki yıldan beş yıla kadar hapis ve adli para cezası ile cezalandırılır.

2. Fiilin; özel nitelikli kişisel verilere, çocuklara ait verilere, kimlik belgesi veya finansal erişim bilgilerine ilişkin olması ya da kritik kamu hizmetinin sürekliliğini somut biçimde tehlikeye düşürmesi halinde ceza yarı oranında artırılır.

3. Fiilin menfaat temini amacıyla, örgüt faaliyeti kapsamında veya çok sayıda kişiyi etkileyen veri setleri üzerinden işlenmesi halinde ceza bir katına kadar artırılır.

4. Failin, verileri erişimden kaldırması, yayılmasını önlemek için makul teknik tedbirleri alması ve mağdur ile yetkili makamlara gecikmeksizin bildirimde bulunması halinde, verilecek cezada üçte birden yarıya kadar indirim yapılabilir.

1.10 Alternatif Hükmün Gerekçesi

Genel amaç, suçun konusunu daha açık hale getirmektedir. Mevcut hükümdeki "daha önce yer alan" ifadesi yerine, verinin bir siber olay veya siber saldırı sonucunda hukuka aykırı olarak elde edilmiş olması şartı öne çıkarılmıştır. Böylece her internet verisinin değil, ihlal kaynaklı verinin hedeflendiği netleşmektedir.

Özel nitelikli kişisel veriler, çocuk verileri, kimlik ve finansal erişim bilgileri ile kritik kamu hizmetine etkisi olan veriler daha ağır yaptırıma bağlanmıştır. Böylece yaptırım, fiilin haksızlık içeriğiyle daha uyumlu hale gelmektedir.

Etkin pişmanlığa benzer bir indirim mekanizması öngörülmüştür. Siber uzayda yayılan verinin tamamen ortadan kaldırılması her zaman mümkün olmasa da failin veriyi kaldırması, yeniden yayılmasını önlemek için teknik tedbir alması ve bildirim yapması zararı azaltabilir. Ceza hukukunun amacı yalnızca cezalandırma değil, zararın büyümesini önleme de olmalıdır.

1.11 Sonuç

7545 sayılı Siber Güvenlik Kanunu m.16/4, güncel siber suç pratiklerine cevap verme ihtiyacından doğmuş önemli bir düzenlemedir. Akira gibi ransomware gruplarının kullandığı çift yönlü şantaj modeli, sızdırılmış verinin sonraki dolaşımının bağımsız bir zarar kaynağı olduğunu göstermektedir. Bu bakımdan hükmün ihdas edilmesi genel olarak isabetlidir.

Ancak ceza hukukunda belirlilik, ölçülülük ve kusur ilkeleri göz ardı edilemez. Hüküm, meşru güvenlik araştırması ve kamu yararı taşıyan açıklamalarla suç oluşturan veri yayma davranışlarını daha açık ayırmalıdır. Ayrıca TCK m.136 ve KVKK ile ilişkisi uygulamada tereddüt yaratmayacak biçimde yorumlanmalı, gerekirse kanun düzeyinde netleştirilmelidir. Bu nedenle mevcut hüküm korunabilir olmakla birlikte, daha açık, kademeli ve istisnaları belirlenmiş bir metinle güçlendirilmesi daha uygun olacaktır.

2 Kaynakça

- 7545 sayılı Siber Güvenlik Kanunu, Resmi Gazete, 19.03.2025, sayı 32846.
- 5237 sayılı Türk Ceza Kanunu.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu.
- Şenol, Cem, “7545 Sayılı Siber Güvenlik Kanunu’nda Düzenlenen Suçlar”, Türkiye Adalet Akademisi Dergisi, 2025.
- Turgut, Bahar, “Siber Uzayda Yer Alan Kişisel veya Kritik Kamu Hizmeti Kapsamına Giren Kurumsal Verileri Erişime Açma, Paylaşma ve Satışa Çıkarma Suçu”, İnönü Üniversitesi Hukuk Fakültesi Dergisi, 2025.