

Kişisel veya Kurumsal Verileri İzinsiz Erişime Açma, Paylaşma veya Satışa Çıkarma Suçu

Siber uzayda yaşanan veri sızıntıları, günümüzün en ciddi bilgi güvenliği sorunlarından birini oluşturmaktadır.

Av. Burak Üçüncü · 6 Haziran 2026 · 10 dk okuma

Siber uzayda yaşanan veri sızıntıları, günümüzün en ciddi bilgi güvenliği sorunlarından birini oluşturmaktadır. Sızıntı sonucu elde edilen verilerin karanlık ağda (dark web) satışa sunulması, hacker forumlarında paylaşılması veya ücretsiz olarak erişime açılması, hem bireylerin temel haklarını hem de kurumların itibarını ve operasyonel güvenliğini doğrudan tehdit etmektedir. 7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin dördüncü fıkrası, bu tehdide karşı spesifik bir ceza normu getirmiştir.

Madde metni şöyledir:

"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 çıkaranlara üç yıldan beş yıla kadar hapis cezası verilir."

Siber güvenlik kanunundaki suçlar arasındaki bu düzenleme, Türk ceza hukuku sisteminde önemli bir boşluğu doldurmaktadır. TCK'nın 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu, genel nitelikteki bir koruma sağlamakla birlikte, siber uzaya özgü veri sızıntısı dinamiklerini yeterince karşılayamamaktaydı. Kanun koyucu, bu fıkayla özellikle veri sızıntısı sonrası gerçekleştirilen ikincil yayma fiillerini hedef almıştır.

BÖLÜM I

Korunan Hukuki Değer

Bu suç tipiyle korunan hukuki değerler çok boyutludur.

Kişisel verilerin korunması hakkı, Anayasa'nın 20. maddesinin üçüncü fıkrasında anayasal güvence altına alınmıştır. Veri sızıntısı sonucu ele geçirilen kişisel verilerin yayılması, bireylerin özel hayatının gizliliğini, kişisel bütünlüğünü ve bilgi kaderini tayin hakkını (informational self-determination) doğrudan ihlal etmektedir. Özellikle sağlık verileri, finansal bilgiler, kimlik numaraları ve iletişim bilgileri gibi hassas verilerin ifşası, kimlik hırsızlığından finansal dolandırıcılığa kadar uzanan bir suç zincirine kaynaklık edebilmektedir.

Kurumsal veri güvenliği de korunan değerler arasındadır. Kritik kamu hizmeti kapsamına giren kurumsal verilerin sızması ve yayılması, kamu hizmetinin sürekliliğini ve güvenilirliğini tehlikeye düşürmektedir. Enerji,

sağlık, ulaşım, finans ve telekomünikasyon gibi sektörlerdeki kurumsal verilerin ifşası, bu altyapıların siber saldırılara karşı savunmasız hale gelmesine yol açabilir.

Son olarak, **siber uzayda kamusal düzen ve güven ortamının korunması** da bu suçun himaye ettiği değerler arasında sayılmalıdır. Sızdırılan verilerin kontrolsüz şekilde dolaşıma girmesi, toplumda genel bir güvensizlik ortamı yaratmakta ve dijital ekonomiye olan inancı zedelemektedir.

BÖLÜM II

Suçun Maddi Unsurları

A. Fail

Suç, herkes tarafından işlenebilen genel bir suçtur (özü suç değildir). Veri sızıntısını bizzat gerçekleştiren kişi ile sızan verileri sonradan yayan kişi farklı kişiler olabilir ve bu fıkra özellikle ikinci gruptaki kişileri hedef almaktadır. Bu ayırım son derece önemlidir: veri sızıntısını gerçekleştiren kişi TCK'nın 243-244. maddelerindeki bilişim suçlarından veya Kanun'un 16/6 hükmünden sorumlu tutulabilecekken, sızan verileri sonradan erişime açan, paylaşan veya satışa çıkaran kişi bu fıkra kapsamında cezalandırılacaktır.

Failin, sızıntıyı gerçekleştiren kişiyle herhangi bir bağlantısının bulunması zorunlu değildir. Sızan verileri internet üzerinden edinen ve bunları yeniden paylaşan herkes bu suçun faili olabilir. Bu kapsamda dark web forumlarında veri setleri satan kişiler, Telegram, Discord veya benzeri platformlarda sızan verileri paylaşan kullanıcılar, sızan verileri derleyerek web sitelerinde yayımlayan kişiler, sızan verileri ücretli veya ücretsiz olarak üçüncü kişilere ileten herkes fail olabilir.

B. Mağdur

Suçun mağduru, kişisel verileri sızan gerçek kişiler ile kurumsal verileri sızan kurumlardır. Madde metninde "kişilerin veya kurumların izni olmaksızın" ifadesiyle mağdur çevresi açıkça belirlenmiştir.

C. Suçun Konusu

Suçun konusu, madde metninde iki kategori halinde belirlenmiştir:

Kişisel veriler: 6698 sayılı KVKK'nın 3. maddesindeki tanım çerçevesinde, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Ad-soyad, T.C. kimlik numarası, adres, telefon numarası, e-posta adresi, finansal bilgiler, sağlık verileri, biyometrik veriler ve benzeri tüm veriler bu kapsamdadır.

Kritik kamu hizmeti kapsamına giren kurumsal veriler: Kanun'un 3. maddesinin (e) bendinde kritik kamu hizmeti, "ulusal, toplumsal veya ekonomik faaliyetlerin sürdürülmesi için gerekli olan ve kesintiye uğraması veya zarar görmesi halinde ulusal güvenlik, ülkenin sosyal veya ekonomik refahı, kamu düzeni veya sağlığı ya da diğer hizmetlerin sunumu üzerinde önemli bir etki oluşturabilecek ülke genelinde tekel veya sınırlı ikame ile sunulan hizmet" olarak tanımlanmıştır. Bu hizmetlere ilişkin kurumsal veriler (örneğin enerji dağıtım şebekesinin yapılandırma verileri, hastane bilgi yönetim sistemi kayıtları veya bankacılık sistemi altyapı bilgileri) suçun konusunu oluşturabilir.

Dikkat çekici bir husus, madde metnindeki "**siber uzayda veri sızıntısı nedeniyle daha önce yer alan**" ifadesidir. Bu ifade, suçun konusunu oluşturan verilerin, daha önceki bir siber olay sonucunda siber uzaya sızmış olmasını ön koşul olarak aramaktadır. Başka bir deyişle, verilerin ilk kez ele geçirilmesi ve sızdırılması

bu fıkra kapsamında değildir; bu fiiller TCK'nın 243-244. maddeleri veya Kanun'un 16/6 hükmü kapsamında değerlendirilecektir. Bu fıkra, yalnızca daha önce sızmış olan verilerin yeniden erişime açılması, paylaşılması veya satışa çıkarılması fiillerini cezalandırmaktadır.

D. Fiil

Suçun maddi unsurunu oluşturan fiil, üç seçimlik hareketle gerçekleştirilebilir:

Erişime açma: Sızan verilerin, belirli veya belirsiz sayıda kişinin erişimine sunulmasıdır. Verilerin bir web sitesinde, dosya paylaşım platformunda veya herhangi bir dijital ortamda erişilebilir hale getirilmesi bu kapsamdadır. Erişime açma, verilerin fiilen indirilmesini veya görüntülenmesini gerektirmez; erişilebilir kılınması yeterlidir.

Paylaşma: Sızan verilerin, belirli kişi veya kişilere aktif olarak iletilmesidir. E-posta, mesajlaşma uygulamaları, dosya transferi veya fiziksel ortamda teslim yoluyla gerçekleştirilebilir. Erişime açmadan farklı olarak, paylaşma belirli muhataplara yönelik bir iletimi ifade etmektedir.

Satışa çıkarma: Sızan verilerin, bedel karşılığında elde edilebilir hale getirilmesidir. Dark web pazaryerlerinde ilan verilmesi, özel satış tekliflerinin sunulması veya açık artırma usulüyle satışa çıkarılması bu kapsamdadır. Satışın fiilen gerçekleşmesi zorunlu değildir; satışa çıkarma fiilinin tamamlanması suçun oluşması için yeterlidir.

Madde metnindeki “**ücretli veya ücretsiz şekilde**” kaydı, failin ekonomik bir menfaat elde edip etmediğinin suçun oluşması bakımından önemsiz olduğunu açıkça ortaya koymaktadır. Verilerin hayırseverlik veya aktivizm gibi motivasyonlarla ücretsiz olarak paylaşılması da suç oluşturmaktadır.

E. Hukuka Aykırılık Unsuru

Madde metninde açıkça “kişilerin veya kurumların izni olmaksızın” ifadesine yer verilmiştir. Dolayısıyla, veri sahibinin rızasının bulunması halinde fiil hukuka uygun hale gelecek ve suç oluşmayacaktır. Ancak uygulamada, veri sızıntısına maruz kalan kişi veya kurumların, sızan verilerinin paylaşılmasına izin vermesi olağan dışı bir durumdur.

Burada önemli bir yorum sorunu ortaya çıkmaktadır: İznin kapsamı nedir? Bir kurumun, güvenlik araştırmaları amacıyla sızan verilerinin incelenmesine izin vermesi, bu verilerin kamuya açık şekilde paylaşılmasına da izin verildiği anlamına gelmez. İznin, paylaşımın yöntemi, kapsamı ve muhatabı bakımından belirli olması aranmalıdır.

BÖLÜM III —

Suçun Manevi Unsuru

Kanun'da özel bir kast türü aranmamış olup, genel kast yeterlidir. Failin; paylaştığı, erişime açtığı veya satışa çıkardığı verilerin, bir siber sızıntı sonucu elde edilmiş kişisel veya kurumsal veriler olduğunu bilmesi ve ilgililerin izninin bulunmadığını bilmesi ya da en azından öngörmesi gerekmektedir.

Olası kast bakımından, failin verilerin sızıntı kaynaklı olabileceğini öngörmesine rağmen bu riski göze alarak paylaşma eylemini gerçekleştirmesi halinde de suçun oluşacağı kabul edilmelidir.

Taksirle işlenme hali düzenlenmemiştir. Dolayısıyla, bir kişinin farkında olmaksızın sızdırılmış verileri paylaşması — örneğin sosyal medyada karşılaştığı bir bağlantıyı içeriğini bilmeden retweetlemesi — bu suçu oluşturmayacaktır.

Failin motivasyonu (maddi kazanç, intikam, aktivizm, merak vb.) suçun oluşmasını etkilemez; ancak cezanın bireyselleştirilmesinde dikkate alınabilir.

BÖLÜM IV

Yaptırım

Suç için öngörülen yaptırım, üç yıldan beş yıla kadar hapis cezasıdır. Sır saklama yükümlülüğü ihlalinde olduğu gibi, burada da adli para cezası öngörülmemiştir.

Alt sınırın üç yıl olması nedeniyle, HAGB uygulanması mümkün değildir (CMK m.231 uyarınca üst sınır iki yıldır). Cezanın ertelenmesi de mümkün değildir (TCK m.51 uyarınca üst sınır iki yıldır). Ayrıca üst sınırdan dolayı tutuklama kararı verilebilir (CMK m.100).

Dolayısıyla bu suçtan mahkum olan failin cezaevine girmesi kaçınılmazdır. Bu durum, özellikle sızıntı verilerini merak veya bilgilendirme amaçlı paylaşan kişiler bakımından ağır sonuçlar doğurabilecektir.

BÖLÜM V

Nitelikli Haller

Kanun'un 16/7 hükmündeki ağırlaştırıcı sebepler bu suç bakımından da geçerlidir:

Kamu görevlisi tarafından işlenmesi: Alt sınır dört yıla yükselir. Bir kamu görevlisinin, göreviyle bağlantılı olarak sızan verilere erişmesi ve bunları paylaşması bu kapsamda değerlendirilebilir.

Birden fazla kişi tarafından birlikte işlenmesi: Alt sınır dört yıl altı aya yükselir. Organize veri ticareti yapan gruplar bakımından bu nitelikli hal sıklıkla uygulama alanı bulabilecektir.

Bir örgütün faaliyeti çerçevesinde işlenmesi: Ceza yarısından iki katına kadar artırılır. Dark web'de organize şekilde veri ticareti yapan yapılar bakımından bu nitelikli halin uygulanması söz konusu olabilecektir. Üst sınır teorik olarak on yıla kadar çıkabilir.

BÖLÜM VI

TCK'daki Benzer Suçlarla İlişkisi

A. TCK m.136 – Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

TCK'nın 136. maddesinde [kişisel verileri](#), hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişilerin cezalandırılacağı düzenlenmiştir. Bu suçun cezası iki yıldan dört yıla kadar hapis cezasıdır.

Kanun'un 16/4 hükmü ile TCK m.136 arasında önemli farklar bulunmaktadır. İlk olarak, Kanun'un 16/4 hükmü yalnızca siber uzayda veri sızıntısı sonucu ortaya çıkan verileri kapsamaktadır; TCK m.136 ise böyle bir sınırlama içermemektedir. İkinci olarak, Kanun'un 16/4 hükmü kişisel verilerin yanı sıra kritik kamu hizmeti kapsamına giren kurumsal verileri de kapsamaktadır; TCK m.136 ise yalnızca kişisel verilerle sınırlıdır. Üçüncü olarak, Kanun'un yaptırımı (3-5 yıl) TCK m.136'daki yaptırımdan (2-4 yıl) daha ağırdır.

Siber uzayda veri sızıntısı sonucu ortaya çıkan kişisel verilerin paylaşılması halinde, her iki suçun unsurları da gerçekleşebilir. Bu durumda, özel norm-genel norm ilişkisi çerçevesinde Kanun'un 16/4 hükmünün öncelikli olarak uygulanması gerekmektedir.

B. TCK m.243-244 – Bilişim Suçları

Veri sızıntısını bizzat gerçekleştiren kişi, TCK'nın 243. maddesindeki bilişim sistemine girme ve 244. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarından sorumlu tutulabilir. Aynı kişinin sızdırdığı verileri sonradan paylaşması veya satışa çıkarması halinde, hem TCK m.243-244 hem de Kanun'un 16/4 hükmü gündeme gelecektir. Bu durumda gerçek içtima uygulanarak her iki suçtan ayrı ayrı ceza verilmesi mümkündür; zira korunan hukuki değerler ve fiiller birbirinden farklıdır.

C. KVKK ile ilişkisi

6698 sayılı KVKK'nın 17. ve 18. maddelerinde düzenlenen yaptırımlar ile Kanun'un 16/4 hükmü arasındaki ilişki de değerlendirilmelidir. KVKK'nın 17. maddesi, kişisel verilere ilişkin suçlar bakımından TCK'nın 135-140. maddelerine atıf yapmaktadır. Kanun'un 16/4 hükmü ise bu genel düzenlemelere ek olarak, siber sızıntı kaynaklı veriler bakımından özel bir norm getirmektedir.

BÖLÜM VII

Uygulamada Karşılaşılabilecek Sorunlar

A. Daha Önce Yer Alan Kavramının Yorumu

Madde metnindeki "siber uzayda veri sızıntısı nedeniyle daha önce yer alan" ifadesi, suçun oluşması için verilerin daha önceki bir sızıntı olayında siber uzaya çıkmış olmasını aramaktadır. Ancak "daha önce yer alan" ifadesinin zamansal kapsamı belirsizdir. Yıllar önce sızmış verilerin yeniden paylaşılması da bu suçu oluşturacak mıdır? Kanaatimizce, zamansal bir sınırlama bulunmadığından, ne zaman sızmış olursa olsun bu verilerin yeniden paylaşılması suç oluşturacaktır.

B. Veri Sızıntısı Olgusunun İspatı

Suçun oluşması için verilerin bir "veri sızıntısı" sonucu siber uzaya çıkmış olması gerekmektedir. Dolayısıyla, verilerin hukuka uygun şekilde kamuya açıklanmış olması halinde bu fıkra uygulanamaz. İspat bakımından, soruşturma makamlarının verilerin gerçekten bir sızıntı olayından kaynaklandığını tespit etmesi gerekecektir. Büyük ölçekli sızıntılarda bu tespit görece kolay olmakla birlikte, küçük ölçekli veya kaynağı belirsiz veri setleri bakımından ispat güçlükleri yaşanabilir.

C. Gazetecilik ve Araştırmacılık Faaliyetleri

Siber güvenlik araştırmacılarının veya gazetecilerin, bir veri sızıntısını haberleştirmek veya analiz etmek amacıyla sızan verilere erişmesi ve bunları belirli ölçüde paylaşması, mesleki faaliyet kapsamında değerlendirilebilir mi? Madde metninde gazetecilik veya araştırma istisnası yer almamaktadır. Bu durum, basın özgürlüğü ve halkın bilgilendirilme hakkı bakımından ciddi endişelere yol açmaktadır.

Özellikle siber güvenlik araştırmacılarının (bug bounty hunters) faaliyetleri bakımından önemli bir sorun mevcuttur. Bir araştırmacının, sızan verilerin varlığını doğrulamak ve sızıntının kapsamını tespit etmek

amacıyla bu verilere erişmesi ve bulgularını raporlaması, suçun unsurlarını teknik olarak karşılayabilir. Bu durum, sorumlu ifşa (responsible disclosure) kültürü bakımından caydırıcı bir etki yaratabilir.

D. Sosyal Medyada Paylaşım

Veri sızıntısı haberlerinin sosyal medyada paylaşılması sırasında, sızan verilerin bir kısmının da paylaşılması oldukça yaygın bir durumdur. Örneğin, bir kullanıcının sızıntıyı kanıtlamak amacıyla birkaç örnek veri kaydını ekran görüntüsü olarak paylaşması, teknik olarak bu suçun unsurlarını karşılayabilir. Bu durumda, paylaşılan verinin miktarı ve niteliği bakımından bir bagatelle (önemsizlik) değerlendirmesi yapılıp yapılamayacağı tartışmalıdır. Türk ceza hukuku sisteminde genel bir bagatelle ilkesi bulunmamakla birlikte, somut tehlike değerlendirmesi çerçevesinde fiilin tipikliğinin sorgulanması mümkün olabilir.

E. Yurt Dışı Bağlantısı

Veri sızıntılarının büyük çoğunluğu uluslararası nitelik taşımaktadır. Sızan verilerin yurt dışındaki sunucularda barındırılması, yabancı uyruklu kişiler tarafından paylaşılması veya yurt dışı platformlarda satışa çıkarılması halinde, yetki alanı (jurisdiction) ve uluslararası adli yardım sorunları gündeme gelecektir. TCK'nın 8. maddesi uyarınca, suçun Türkiye'de veya Türk vatandaşına karşı işlenmesi halinde Türk mahkemelerinin yetkisi kabul edilmektedir; ancak failin yurt dışında bulunması halinde fiili yargılamanın gerçekleştirilmesi önemli güçlükler içermektedir.

BÖLÜM VIII

Sonuç

7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin dördüncü fıkrası, siber uzaydaki veri sızıntılarının ikincil zararlarını (yani sızan verilerin yayılması, paylaşılması ve ticaretini) hedef alan özgün bir suç tipidir. Türk ceza hukuku sisteminde bu alanda var olan boşluğu doldurmakta ve özellikle TCK m.136'daki düzenlemeyi siber uzaya özgü koşullar bakımından tamamlamaktadır.

Suçun geniş kapsamı, üç yıldan beş yıla kadar hapis cezası öngörmesi ve HAGB ile erteleme imkanının bulunmaması, kanun koyucunun bu alandaki caydırıcılık iradesini yansıtmaktadır. Ancak gazetecilik faaliyetleri, güvenlik araştırmacılığı ve sosyal medya paylaşımları gibi konularda ortaya çıkabilecek orantılılık sorunlarının, içtihatlarla ve mümkünse ikincil mevzuatla çözümlenmesi gerekmektedir. Bu suç tipinin manevi unsurundaki karmaşık yapı (özel bilgi ve özel amaç gereksinimi) soruşturma ve kovuşturma aşamalarında ciddi savunma stratejileri gerektirmekte olup, şüpheli veya sanıkların sürecin en başından itibaren siber güvenlik mevzuatına hakim bir **bilişim suçları avukatı**ndan hukuki destek alması büyük önem taşımaktadır.

Veri sızıntılarının artış gösterdiği günümüzde, bu suç tipinin etkin şekilde uygulanması, hem bireylerin kişisel verilerinin korunması hem de kritik kamu hizmetlerinin güvenliği bakımından hayati önem taşımaktadır. Bununla birlikte, uygulamanın temel hak ve özgürlüklerle dengelenmesi, hukuk devleti ilkesinin vazgeçilmez bir gereğidir.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/kisisel-veya-kurumsal-verileri-izinsiz-erisime-acma-paylasma-veya-satisa-cikarma-sucu>