

Yasadışı Sorgu Panelleri – Suçlar ve Cezalar

Av. Burak Üçüncü · 14 Mayıs 2026 · 8 dk okumaGüncelleme: 17 Temmuz 2026

Bir kişinin TC kimlik numarasını yazıp birkaç saniye içinde adresine, telefon numarasına, tapu kaydına, aile bilgilerine ve hatta vesikalık fotoğrafına ulaşabildiğiniz bir sistem düşünün. Üstelik bunu yapabilmek için ne bir devlet kurumunda çalışıyor olmanız ne de herhangi bir hukuksal yetkiye sahip olmanız gerekiyor. Tek ihtiyacınız birkaç yüz liralık bir üyelik paketi ve bir Telegram hesabı. İşte Türkiye’de sorgu paneli olarak bilinen yasadışı sistemlerin sunduğu tam olarak budur.

Peki bu panelleri kurmak, işletmek veya bu sürecin herhangi bir halkasında yer almak hukuki açıdan ne anlama geliyor? Cumhuriyet savcılıkları bu faaliyetlere nasıl bakıyor, hangi suçları oluşturduğunu değerlendiriyor ve hangi delillere dayanıyor? Bu yazıda, yasadışı panel işletmenin cezai boyutunu tüm yönleriyle ele alacağız. Siber suç cezası denildiğinde akla yalnızca bireysel hacking faaliyetleri gelebilir; ancak panel işletme, çok daha katmanlı ve ağır yaptırımları olan bir suç kategorisidir.

BÖLÜM II

Sorgu Paneli Nedir?

Türkiye’de son birkaç yılda siber suç dünyasının en hızlı büyüyen ve en tehlikeli segmentlerinden biri haline gelen sorgu panelleri, aslında teknik olarak oldukça basit bir mantıkla çalışan sistemlerdir. Çeşitli kaynaklardan (kişisel veri ihlalleri, sızıntılar, siber saldırılar, dark web üzerinden satın alınan veya indirilen veri setleri veya kamu kurumlarının bilişim sistemlerine yetkisiz erişim yoluyla) elde edilen kişisel veriler bir araya getirilir, bir veri tabanında birleştirilir ve genelde bir web arayüzü ya da Telegram botu aracılığıyla kullanıcıların erişimine sunulur.

Kullanıcı, panele bir TC kimlik numarası, ad-soyad veya telefon numarası girer; karşısına o kişiye ait kimlik bilgileri, aile bilgileri, nüfus kayıtları, adres, telefon numarası, tapu kaydı, SGK kaydı, hatta fotoğraf gibi kişisel veriler çıkar. Bu hizmet genellikle tek seferlik, haftalık, aylık, yıllık veya sınırsız paketler halinde satışa sunulur. Ödeme yöntemi olarak kişisel banka hesapları, başkalarının adına açılmış hesaplar, elektronik para kuruluşları ve kripto para cüzdanları kullanılır.

Bu panellerin boyutu küçümsenecek gibi değildir. Günümüzde tespit edilen panellerin sunucularında 100 milyonun üzerinde kimlik kaydı, 100 milyonu aşkın GSM verisi, onlarca milyon tapu ve SGK kaydı barındırılmaktadır. Türkiye’nin toplam nüfusunun yaklaşık 85 milyon olduğu düşünüldüğünde, bu rakamların pratikte tüm vatandaşların verilerini kapsadığı tahmin edilmektedir.

BÖLÜM III

Paneller Nasıl Çalışıyor?

Bir sorgu panelinin teknik altyapısını anlamak, işlenen suçların niteliğini kavramak açısından önemlidir. Paneller genellikle şu bileşenlerden oluşur.

Veri tabanı katmanı

Panelin temelini oluşturan kısımdır. Farklı kaynaklardan temin edilen veriler (kimlik bilgileri, GSM kayıtları, adres bilgileri, tapu verileri, SGK kayıtları) ayrı tablolar halinde bir veya birden fazla veri tabanında tutulur. Bu veri tabanlarının boyutu yüzlerce milyon satıra ulaşabilir.

API bağlantıları

Panellerin bir kısmı yalnızca statik verilerle çalışmaz. Bazı paneller, kamu kurumlarının bilişim sistemlerine API bağlantısı kurarak anlık veri çekme kapasitesine sahiptir. Örneğin, bir kişinin güncel adres bilgisini Gelir İdaresi Başkanlığı'nın sisteminden, tapu bilgisini Tapu ve Kadastro Genel Müdürlüğü'nün sisteminden anlık olarak sorgulayabilirler. Bu durum, panelin tehlike seviyesini katbekat artırır; çünkü artık yalnızca geçmişte sızdırılmış verilerden değil, devletin canlı sistemlerinden veri akışı söz konusudur.

Web arayüzü ve botlar

Veriler, kullanıcı dostu bir web sitesi üzerinden ya da Telegram gibi mesajlaşma platformlarında çalışan otomatik botlar aracılığıyla sunulur. Kullanıcı, basit bir form doldurarak veya bota bir komut göndererek sorgulama yapabilir. Panellerin bir kısmı giriş anahtarı veya davet kodu sistemiyle çalışır.

Satış ve tanıtım altyapısı

Panel sahipleri, Telegram kanalları ve grupları üzerinden reklam yapar, üyelik paketlerini duyurur ve müşteri desteği sağlar. Satış genellikle kripto para veya elektronik para kuruluşları üzerinden yapılır. Banka hesapları da kullanılmakla birlikte, bu hesaplar genellikle başka kişilerin adına kayıtlıdır veya para transferine katman oluşturmak amacıyla kullanılır.

Sunucu altyapısı

Panellerin kaynak kodları ve verileri genellikle yurt dışı lokasyonlu VPS/VDS sunucularda barındırılır. Ancak Türkiye merkezli hosting firmalarından da sunucu satın alındığı görülmektedir. Sunucu satın alma işlemleri çoğunlukla sahte isimlerle, başkalarına ait iletişim ve kart bilgileriyle ve sanal POS üzerinden gerçekleştirilir.

BÖLÜM IV

Savcılıklar Meseleye Nasıl Bakıyor?

Cumhuriyet savcılıkları, yasadışı panel işletme faaliyetini tek bir suç olarak değil, birden fazla suçun bir arada işlendiği karmaşık bir eylem bütünü olarak değerlendirmektedir. Bu yaklaşım, panelin teknik yapısının ve işleyişinin farklı suç tiplerini aynı anda bünyesinde barındırmasından kaynaklanmaktadır. Savcılık pratiğinde panel işletme genellikle üç ana suç kategorisi üzerinden ele alınır.

Birinci Kategori: Siber Güvenlik Kanunu Kapsamında Değerlendirme

19 Mart 2025 tarihinde yürürlüğe giren 7545 sayılı [Siber Güvenlik Kanunu](#), Türkiye'nin bu alandaki ilk kapsamlı yasal düzenlemesidir. Kanunun 16. maddesinin 6. fıkrası, siber suç faaliyetlerinin organize şekilde

yürütülmesine yönelik ağırlaştırılmış cezai yaptırımlar öngörmektedir.

Savcılıklar, panel işletme faaliyetlerini bu kanun kapsamında değerlendirirken özellikle şu unsurlara dikkat etmektedir. Faaliyetin birden fazla kişi tarafından yürütülüp yürütülmediği, şüpheliler arasında bir görev dağılımı olup olmadığı, faaliyetin süreklilik arz edip etmediği ve ekonomik bir motivasyonla hareket edilip edilmediği. Panel işletme faaliyetlerinde neredeyse her zaman bir organizasyon yapısı bulunmaktadır. Yazılımı geliştiren, satışı yapan, parayı toplayan ve dağıtan, veri temin eden farklı kişiler mevcuttur. Bu durum, Siber Güvenlik Kanunu'nun ağırlaştırılmış hükümlerinin uygulanmasına zemin hazırlamaktadır.

Kanunun yürürlüğe girmesinden bu yana, panel davalarında bu maddeye atıf yapılması standart bir uygulama haline gelmiştir. Bu, faillerin yalnızca TCK hükümleriyle değil, özel bir kanunun ağırlaştırılmış yaptırımlarıyla da karşı karşıya kalması anlamına gelmektedir.

İkinci Kategori: TCK 244 – Bilişim Sistemindeki Verileri Bozma, Yok Etme, Sisteme Veri Yerleştirme

Türk Ceza Kanunu'nun 244. maddesi, bilişim sistemlerindeki verilere yönelik müdahaleleri cezalandırmaktadır. Maddenin ikinci fıkrası, bir bilişim sistemindeki verileri bozan, yok eden, değiştiren, erişilmez kılan, sisteme veri yerleştiren veya var olan verileri başka bir yere gönderen kişiyi cezalandırır. Üçüncü fıkra ise bu fiillerin bir banka, kredi kurumu veya kamu kurum ya da kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde cezanın yarı oranında artırılmasını öngörür.

Panel davalarında savcılıkların bu madde değerlendirmesi, özellikle panelin kamu kurumlarının sistemlerine yetkisiz erişim sağladığının tespit edilmesi halinde gündeme gelir. Burada dikkat çekici bir uygulama söz konusudur. Savcılıklar, her bir kamu kurumuna yönelik erişimi ayrı bir suç olarak değerlendirme eğilimindedir. Yani bir panel hem Gelir İdaresi Başkanlığı'nın hem de Tapu ve Kadastro Genel Müdürlüğü'nün sistemine erişim sağlıyorsa, genelde bu iki ayrı TCK 244 suçu olarak nitelendirilmekte ve bu yönde cezalandırma istemektedir.

Bu noktada statik veri ile anlık erişim arasındaki fark kritiktir. Bir panelin yalnızca daha önce sızdırılmış verileri barındırması ile bir kamu kurumunun canlı sistemine API bağlantısı kurarak anlık veri çekmesi, hukuki değerlendirme açısından tamamen farklı sonuçlar doğurur. İkinci durum, TCK 244'ün ağırlaştırılmış halini tetikler ve suçun süregelen niteliğini ortaya koyar.

Savcılıklar, sunucu incelemelerinde kaynak kodları analiz ettirerek panelin hangi kamu kurumlarına bağlantı kurduğunu tespit ettirmektedir. Genellikle USOM (Ulusal Siber Olaylara Müdahale Merkezi) tarafından hazırlanan teknik inceleme raporları, bu tespitlerin temel dayanağını oluşturmaktadır.

Üçüncü Kategori: TCK 136 – Kişisel Verileri Hukuka Aykırı Olarak Ele Geçirmek veya Yaymak

TCK'nın 136. maddesi, kişisel verileri hukuka aykırı olarak ele geçiren, yayan veya bir başkasına veren kişiyi cezalandırmaktadır. Panel davalarında bu maddenin, neredeyse istisnasız olarak TCK 43/1 (zincirleme suç) hükmüyle birlikte uygulanması talep edilmektedir. Bunun nedeni açıktır, panel işletmecileri tek bir kişinin değil, milyonlarca kişinin verilerini aynı suç işleme kararı kapsamında ele geçirip yaymaktadır.

Savcılıkların bu suçu değerlendirirken baktığı temel unsurlar şunlardır. Verilerin kapsamı (hangi tür veriler ele geçirilmiş (kimlik, adres, telefon, tapu, SGK vb.), verilerin miktarı (kaç kişiye ait verinin ele geçirildiği),

verilerin yayılma biçimi (web sitesi, Telegram botu, doğrudan satış vb.) ve verilerin ticari amaçla kullanılıp kullanılmadığı.

Panel davalarında zincirleme suç uygulaması, ceza miktarını önemli ölçüde artıran bir faktördür. TCK 43/1'e göre, bir suçun zincirleme olarak işlenmesi halinde ceza dörtte birinden dörtte üçüne kadar artırılır. Yüz milyonlarca kişiye ait verinin sistematik şekilde ele geçirilip yayılması, bu artırımın üst sınıra yakın uygulanmasını haklı kılabilen bir ölçek olup risk unsurunu artırmaktadır.

BÖLÜM V

Genel Tablo ve Sonuç

Panel davalarında en dikkat çekici eğilimlerden biri, şüphelilerin büyük çoğunluğunun 16-22 yaş aralığında olmasıdır. Siber suçlar giderek daha genç yaş gruplarına yayılmakta, teknik bilgi sahibi gençler kolay para motivasyonu bu faaliyetlere yönelmektedir. Şüphelilerin bir kısmının suç tarihinde henüz 18 yaşından küçük olması, çocuk ceza hukuku kapsamında ayrı bir değerlendirmeyi de gündeme getirmektedir. Ancak yaş küçüklüğü, suçun niteliğini değiştirmemekte; savcılıklar bu dosyalarda da aynı sevk maddelerini uygulamaktadır.

Soruşturmalarda sıklıkla karşılaşılan bir diğer durum, aynı şüpheli grubunun birden fazla panel kurmuş olmasıdır. Bir panel kapatıldığında veya tespit edildiğinde, aynı altyapı ve verilerle farklı isimler altında yeni paneller kurulması yaygın bir pratiktir. Bu durum, faaliyetin süreklilik ve kararlılık arz ettiğini göstermesi bakımından savcılıklar tarafından özellikle vurgulanmaktadır. Panel gelirlerinin toplanması ve dağıtılmasında da giderek daha sofistike yöntemler kullanılmaktadır. Doğrudan banka havalesi yerine kripto para cüzdanları, elektronik para kuruluşları ve başkalarının adına açılmış hesaplar üzerinden katmanlı bir ödeme sistemi kurulması yaygınlaşmıştır. Paranın birden fazla hesap üzerinden geçirilerek iz sürmeyi zorlaştırma çabası, MASAK tarafından katman oluşturma olarak nitelendirilmekte ve kara para aklama bağlamında ayrıca değerlendirilebilmektedir. Buna ek olarak, panel operasyonlarında şüpheliler arasında belirgin bir uzmanlaşma ve görev dağılımı bulunmaktadır. Yazılım geliştirme, veri temini, API entegrasyonu, satış, tanıtım ve mali operasyonlar farklı kişiler tarafından üstlenilmekte; hatta bazı şüpheliler yalnızca kendi adlarına kayıtlı banka veya kripto hesaplarını panel operatörlerinin kullanımına sunma rolünü üstlenmektedir. Savcılıklar, bu tür rolleri de iştirak kapsamında değerlendirmektedir.

Tüm bu suç tiplerini ve ağırlaştırıcı sebepleri bir arada değerlendirdiğimizde ortaya ciddi bir tablo çıkmaktadır. Siber Güvenlik Kanunu'nun ilgili maddesi, TCK 244'ün birden fazla kamu kurumuna karşı işlenmesi nedeniyle her bir kurum için ayrı ceza, TCK 136'nın zincirleme suç hükmüyle birlikte uygulanması ve TCK 53 kapsamında hak yoksunlukları bir araya geldiğinde, toplam ceza miktarı yıllarla ifade edilen seviyelere ulaşabilmektedir. Üstelik bu cezalar her bir şüpheli için ayrı ayrı uygulanmaktadır; panel operasyonuna herhangi bir aşamada katılmış olan herkes, aynı suçlardan dolayı ayrı ayrı yargılanmakta ve cezalandırılmaktadır.

Sonuç olarak yasadışı panel işletme, Türk ceza hukuku açısından çok katmanlı ve son derece ağır yaptırımları olan bir suç faaliyetidir. Bu tür dosyalarda etkin bir savunma stratejisi geliştirebilmek için teknik altyapıyı anlayan bir [bilişim hukuku avukatı](#) ile çalışmak büyük önem taşımaktadır. 7545 sayılı Siber Güvenlik Kanunu'nun yürürlüğe girmesiyle birlikte bu alandaki cezai yaptırımlar daha da sertleşmiş, savcılıkların ve kolluk kuvvetlerinin teknik soruşturma kapasitesi önemli ölçüde artmıştır. USOM teknik raporları, MASAK mali analizleri, telekomünikasyon verileri ve platform yazışmaları gibi çok katmanlı delil yapıları sayesinde,

dijital ortamda anonimlik sağladığını düşünen faillerin gerçek kimliklerine ulaşmak artık çok daha mümkündür. Panel kurmak, işletmek, tanıtmak, satış yapmak, veri temin etmek, hesap kiralamak veya mali altyapıyı sağlamak bu sürecin herhangi bir halkasında yer almak, ağır cezai sorumluluk doğurmaktadır. Özellikle genç yaştaki bireylerin teknik merak veya kolay kazanç motivasyonu ile bu faaliyetlere yönelmesi, hem bireysel hem de toplumsal açıdan ciddi sonuçlar doğurabilecek bir risk alanı oluşturmaktadır.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/yasadisi-sorgu-panelleri-suclar-ve-cezalar>