KİŞİSEL VERİLERİN KORUNMASI SİBER GÜVENLİK SUÇLARI

Bilgilerim Sorgu Panelinde Çıkıyor, Ne Yapmalıyım?

Av. Burak Üçüncü · 15 Kasım 2026 · 10 dk okuma

Bir tanıdığın gönderdiği ekran görüntüsünde kendi adınızı, T.C. kimlik numaranızı, adresinizi, anne ve baba adınızı, hatta kayıtlı telefon hatlarınızı görmek ciddi bir tedirginlik yaratır. Sorgu panelleri, farklı kurum ve şirketlerden sızdırılmış veri tabanlarını birleştirerek bir kişinin adı veya kimlik numarasıyla aranabilir hale getiren yasa dışı hizmetlerdir. Panelin işleyişi, kimlerin hangi suçtan sorumlu tutulduğu ve uygulanan cezalar sorgu panellerine ilişkin ayrıntılı yazıda ele alınmıştır. Bu yazı ise meseleye verisi panelde yer alan kişinin gözünden bakmaktadır.

Başlangıçta vurgulanması gereken husus, bir kişinin bilgilerinin panelde çıkmasının o kişi bakımından herhangi bir sorumluluk doğurmadığıdır. Panelde yer alan kişi suçun faili değil mağdurudur. Bu sıfat, hem ceza soruşturmasında hem de kişisel verilerin korunması hukukunda belirli haklar tanır. Aşağıda bu hakların neler olduğu, hangi sırayla kullanılması gerektiği ve verilerin kötüye kullanılmasına karşı alınabilecek önlemler incelenmektedir.

BÖLÜM I

Veriler Panele Nasıl Ulaşır?

Sorgu panellerinde yer alan veriler çoğunlukla tek bir kaynaktan gelmez. Bir kısmı geçmiş yıllarda yaşanan büyük veri sızıntılarından, bir kısmı bir sağlık kuruluşu, operatör bayisi, kargo şirketi veya e-ticaret sitesi gibi veri sorumlularının yetersiz güvenlik önlemlerinden, bir kısmı da yetkili erişimi bulunan kişilerin bu yetkiyi kötüye kullanmasından kaynaklanır. Panel işletenler bu dağınık kayıtları birleştirerek kimlik, adres, aile, telefon, araç ve tapu gibi bilgileri tek bir sorguyla sunar.

Panellerden sorgu yapan kişilerin amaçları da çeşitlidir. Bir kısmı borçlu veya eski eşin adresini bulmak, bir kısmı tanımadığı bir kişi hakkında bilgi toplamak, bir kısmı ise şantaj, ısrarlı takip veya dolandırıcılık için hazırlık yapmak amacıyla panele başvurur. Panelde görünen bilgilerin bir bölümü güncel olmayabilir ya da başka kişilerin kayıtlarıyla karışmış olabilir. Bu nedenle mağdurun, panelde gördüğü her bilgiyi doğru kabul etmeden, özellikle adres ve telefon gibi kendisine ulaşılmasını sağlayan verilerin güncel olup olmadığını değerlendirmesi, risk düzeyini belirlemek bakımından önemlidir.

Bu yapı mağdur bakımından iki sonuç doğurur. Birincisi, verinin hangi kurumdan çıktığını tespit etmek çoğu zaman güçtür ve teknik inceleme gerektirir. İkincisi, aynı veri birden fazla panelde ve uzun süre dolaşımda kalabilir. Bu nedenle mağdurun izleyeceği yol yalnız panelin kapatılmasına değil, sorumluların tespitine, verinin kaynağına ulaşılmasına ve verinin kötüye kullanılmasının önlenmesine yönelik olmalıdır.

BÖLÜM II

Hangi Suçlar Gündeme Gelir?

Mağdur bakımından temel suç tipi Türk Ceza Kanunu'nun 136. maddesinde düzenlenmiştir. Hükme göre kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. Paneli işleten, veriyi panele aktaran ve panelden kendi bilgisi dışındaki kişilere ait verileri sorgulayıp alan kişiler bu üç seçimlik hareketten en az birini gerçekleştirmiş olabilir.

Ele geçirme kavramının sınırları Yargıtay kararlarında belirginleşmiştir. Yargıtay, kurumu tarafından kendisine verilen yetkiyle sistemdeki verilere yalnızca bakan kamu görevlisinin eylemini suç saymamış, bu sonuca varırken ele geçirmenin anlamını *"ele geçirme başkasının hakimiyeti altında bulunan kişisel veriyi hukuka aykırı yollarla kendi hakimiyeti altına almakla gerçekleşir"* sözleriyle açıklamıştır (Yargıtay 12. Ceza Dairesi, 12.05.2025, E. 2025/449, K. 2025/4296). Daire aynı kararda, sistemde görev gereği erişim yetkisi bulunan kişilerin merak gibi saiklerle verilere *"salt duyu organları aracılığıyla vakıf olmaktan ibaret"* eylemlerinin disiplin soruşturmasına konu olabileceğini, ancak suç oluşturmayacağını belirtmiştir.

Bu ayrım sorgu panelleri bakımından önemlidir. Panel kullanıcısının sorguladığı veriler onun kendi hakimiyeti altında bulunan veriler değildir. Kullanıcı, erişim yetkisi bulunmayan bir veri yığınından başkasına ait kayıtları çekip kendi hakimiyetine almaktadır. Bu nedenle panel üzerinden yapılan sorgu, kendi sistemine yetkili erişimi olan görevlinin bakmasından farklı olarak ele geçirme kapsamında değerlendirilmeye elverişlidir. Sınar'ın da vurguladığı gibi TCK m. 136'daki verme, yayma ve ele geçirme hareketleri seçimliktir ve bunlardan birinin gerçekleştirilmesi suçun oluşması için yeterlidir (Sınar, s. 41). Tüzün Karakoçak da gizli sosyal medya profillerindeki içerikleri alıp herkesin görebileceği bir ortamda tutan uygulamaların TCK m. 136 bakımından değerlendirilmesi gerektiğini ve bu uygulamaların yalnız görüntülenen kişilerin değil uygulamayı indirenlerin verilerini de ihlal ettiğini belirtmektedir (Tüzün Karakoçak, s. 426). Sorgu panelleri bu uygulamaların çok daha kapsamlı bir türüdür.

Yetkili erişimin sınırı Ceza Genel Kurulu kararıyla da çizilmiştir. Kurumu tarafından verilen şifreyle Kimlik Paylaşım Sistemi'ne girip dönemin bir bakanının kimlik ve adres bilgilerine merak saikiyle bakan ve bunları kimseyle paylaşmayan memurun eylemi suç sayılmamış, Yargıtay 12. Ceza Dairesi de bu kararı esas alarak SGK sisteminde katılanın bilgilerini yalnız ekranda okuyan görevli hakkındaki beraat kararını onamıştır (Yargıtay 12. Ceza Dairesi, 23.06.2025, E. 2025/361, K. 2025/5540). Buna karşılık sorgulanan bilgilerin üçüncü bir kişiye verilmesi sonucu değiştirir. Katılanın eski sevgilisinin, katılanın konakladığı yerleri, kiraladığı araçları, telefon, UYAP, tapu, pasaport ve SGK kayıtlarını bildiğinin anlaşılması üzerine yapılan araştırmada bu bilgileri sorgulayan görevlinin TCK m. 136 ve 137/1-a uyarınca mahkumiyetine ilişkin hüküm onanmıştır (Yargıtay 12. Ceza Dairesi, 07.04.2026, E. 2025/8484, K. 2026/3419). Panellerdeki verilerin önemli bir kısmı da bu şekilde, yetkili erişimi olan kişilerin sorguladığı kayıtların dışarı aktarılmasıyla oluşur. Verinin panele aktarılmasında yetkisini kötüye kullanan bir kamu görevlisinin veya belirli bir mesleğin sağladığı kolaylıktan yararlanan bir kişinin payı varsa, TCK m. 137 uyarınca ceza yarı oranında artırılır. Yaşar, mesleğin sağladığı kolaylıkla bir veri tabanına erişip görevi dışında kişisel veri ele geçirmenin de bu nitelikli hali oluşturduğunu belirtmektedir (Yaşar, s. 97).

Her sorgu ve aktarım ise kendiliğinden suç değildir. Yargıtay, bir belediye çalışanının iki üst amirinin tapu bilgilerini sorgulayıp usulsüzlük şüphesiyle yalnızca belediye başkanına bildirdiği olayda, bilgilerin üçüncü kişilerle paylaşılmadığını ve hukuka aykırılık bilinciyle hareket edilmediğini kabul eden beraat kararını onamıştır (Yargıtay 12. Ceza Dairesi, 05.01.2026, E. 2025/2253, K. 2026/27). Panel işletenlerin ve aboneliğe

dayalı sorgu yapanların durumu bu kararlardan açıkça ayrılır. Bu kişilerin ne bir görev yetkisi ne de hukuka uygunluk sebebi oluşturacak bir amacı vardır.

Panel işletenler bakımından ayrıca 7545 sayılı Siber Güvenlik Kanunu devreye girer. Kanunun 16. maddesinin dördüncü fıkrası, siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel verileri kişilerin izni olmaksızın ücretli veya ücretsiz şekilde erişime açan, paylaşan veya satışa çıkaranlara üç yıldan beş yıla kadar hapis cezası öngörür. Fıkra, sızıntı yoluyla dolaşıma girmiş verilerin yeniden piyasaya sunulmasını doğrudan hedef aldığı için panellerin işleyişiyle örtüşmektedir. Aynı maddenin yedinci fıkrasına göre suçun birden fazla kişi tarafından işlenmesi halinde ceza yarı oranında, bir örgütün faaliyeti çerçevesinde işlenmesi halinde yarısından iki katına kadar artırılır. Bu suçlar siber güvenlik suçları arasında yer alır ve TCK'daki kişisel veri suçlarıyla birlikte değerlendirilir. Panel işletenlerin sızdırılmış kayıtları kendi sunucularında veya bulut depolama alanlarında toplaması, TCK m. 135'teki kişisel verilerin kaydedilmesi suçu bakımından da ayrıca değerlendirilebilir. Topuz, kaydetmenin hangi araçla ve nereye yapıldığının önem taşımadığını, bulut depolama alanlarının da kayıt yeri olabileceğini belirtmektedir (Topuz, s. 106).

Mağdur açısından pratik sonucu olan bir başka düzenleme TCK m. 139'dur. Bu hükme göre kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme suçları şikayete bağlı değildir. Cumhuriyet savcılığı suçu öğrendiğinde resen soruşturma yapar, mağdurun şikayetinden vazgeçmesi soruşturmayı sona erdirmez. Ancak panelde kimlik bilgileriyle birlikte kişinin özel hayatına ilişkin görüntü veya sesleri de yayılmışsa durum değişebilir. Yargıtay, eylemin özel hayata ilişkin görüntü ve seslerin ifşası niteliğinde olduğu bir dosyada suçu TCK m. 134/2 kapsamında nitelendiren ve şikayetten vazgeçme nedeniyle davanın düşmesine karar veren bölge adliye mahkemesi kararını onamıştır (Yargıtay 12. Ceza Dairesi, 13.04.2026, E. 2024/1437, K. 2026/3678). Bu nitelendirme şikayete bağlı suçlar bakımından altı aylık şikayet süresinin kaçırılmaması gerektiğini de gösterir.

BÖLÜM III

Delillerin Korunması ve Suç Duyurusu

Mağdurun ilk işi panelde görünen bilgilerin kaydını eksiksiz tutmaktır. Ekran görüntüsü, panelin adı veya alan adı, paylaşıldığı Telegram kanalı ya da grubu, sorgunun yapıldığı tarih, görüntüyü gönderen kişinin kimliği ve bu kişinin görüntüye nasıl ulaştığına ilişkin açıklama birlikte saklanmalıdır. Ancak ekran görüntüsünün tek başına delil değeri sınırlıdır. Görüntünün alındığı cihaz, dosyanın özgün hali ve tanık beyanı, soruşturmada görüntünün doğruluğunu destekleyen unsurlar olarak korunmalıdır. Panel hala erişilebilir durumdaysa noter veya bilirkişi aracılığıyla tespit yaptırılması da düşünülebilir.

Suç duyurusu Cumhuriyet başsavcılığına yapılır. Büyük adliyelerde bu tür dosyalar genellikle bilişim suçları bürolarında incelenir. Dilekçede panelde görünen veri türlerinin ayrı ayrı belirtilmesi, panelin erişim adresi, varsa abonelik veya ödeme sayfasındaki banka ve kripto cüzdan bilgileri ile panelin tanıtıldığı kanalların gösterilmesi soruşturmanın yönünü belirler. Panellerin önemli bir kısmı abonelik usulüyle satıldığı için ödeme izleri faillere ulaşmada çoğu zaman alan adı bilgilerinden daha verimlidir. Mağdur ayrıca soruşturmada verinin hangi kaynaktan sızdığının araştırılmasını talep edebilir. Bu araştırma, aşağıda anlatılan veri sorumlusuna karşı idari yol ve tazminat davası bakımından da belirleyicidir.

BÖLÜM IV

Verinin Kaynağına Karşı Başvuru Yolları

Verinin hangi kurumdan çıktığı tespit edilebiliyorsa 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun sağladığı yollar kullanılabilir. Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almakla yükümlüdür (KVKK m. 12/1). İşlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde veri sorumlusu bu durumu en kısa sürede ilgili kişiye ve Kişisel Verileri Koruma Kurulu'na bildirmek zorundadır (KVKK m. 12/5). Bu bildirimin yapılmamış olması başlı başına bir yükümlülük ihlalidir. Kaya, bildirim yükümlülüğünü veri sorumlusunun kendi ihlalini açıklaması olarak nitelendirmekte (Kaya, s. 197) ve ağır yaptırım korkusunun veri sorumlularını ihlali bildirmek yerine delilleri gizlemeye yöneltebileceğine dikkat çekmektedir (Kaya, s. 239). Mağdur bakımından bunun pratik sonucu, veri sorumlusuna yapılan başvuruda bir ihlal bildirimi yapılıp yapılmadığının açıkça sorulmasıdır. Kurul'un 2019/271 sayılı kararına göre ilgili kişiye yapılacak bildirimde ihlalin ne zaman gerçekleştiği, hangi veri kategorilerinin etkilendiği, ihlalin olası sonuçları, alınan veya alınacak tedbirler ve bilgi alınabilecek irtibat kanalları asgari olarak yer almalıdır (Yıldız, s. 72).

İlgili kişi önce veri sorumlusuna yazılı olarak başvurur ve hakkında hangi verilerin işlendiğini, bu verilerin kimlere aktarıldığını ve bir ihlal yaşanıp yaşanmadığını sorar. Veri sorumlusu başvuruyu en geç otuz gün içinde ücretsiz olarak sonuçlandırır (KVKK m. 13/2). Başvurunun reddedilmesi, cevabın yetersiz bulunması veya süresinde cevap verilmemesi halinde, cevabın öğrenildiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikayette bulunulabilir (KVKK m. 14/1). Sürelerin ve dilekçenin ayrıntısı KVKK'ya şikayet sürecini anlatan yazıda yer almaktadır. Kurul, yükümlülüklerini yerine getirmeyen veri sorumlusuna idari para cezası verebilir. Ancak Kurul tazminata hükmetmez ve verilen ceza mağdura değil devlete ödenir.

BÖLÜM V

Verilerin Kötüye Kullanılmasına Karşı Önlemler

Panelde yer alan bilgilerin asıl tehlikesi, dolandırıcılık ve kimlik taklidi için hazır bir altyapı oluşturmasıdır. Kimlik numarası, anne adı ve adres bilgisine sahip bir kişi, kendisini banka, operatör ya da kamu görevlisi olarak tanıtarak mağdura güvenilir görünebilir. Bu nedenle verisinin panelde yer aldığını öğrenen kişinin, kendisini arayan ve kimlik bilgilerini doğru şekilde söyleyen kişilere bu bilgiye dayanarak güvenmemesi gerekir. Şifre, doğrulama kodu ve kart bilgisi hiçbir koşulda telefonda paylaşılmamalıdır.

Bunun yanında e-Devlet şifresinin ve bankacılık şifrelerinin değiştirilmesi, iki aşamalı doğrulamanın açılması, e-Devlet üzerinden adına kayıtlı mobil hatların kontrol edilmesi ve bankaların sunduğu işlem bildirimlerinin etkinleştirilmesi yerinde olur. Adına bilgisi dışında hat açıldığı, hesap veya kredi başvurusu yapıldığı anlaşılırsa ilgili kuruma derhal yazılı bildirim yapılmalı ve bu durum suç duyurusu dosyasına eklenmelidir. Bu bildirimler, ileride bir borç veya işlemle karşılaşıldığında mağdurun işlemden haberdar olmadığını gösteren önemli belgelerdir.

BÖLÜM VI

Tazminat Hakkı

Ceza soruşturması ve idari başvuru mağdurun zararını kendiliğinden gidermez. KVKK m. 14/3, kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı olduğunu belirtir. Türk Medeni Kanunu'nun 24

ve 25. maddeleri, hukuka aykırı olarak kişilik hakkına saldırılan kişiye saldırının durdurulmasını ve hukuka aykırılığın tespitini isteme imkanı tanır, maddi ve manevi tazminat istemlerini saklı tutar. Manevi tazminatın dayanağı Türk Borçlar Kanunu'nun 58. maddesidir.

Tazminat davası panel işletenlere karşı ancak bu kişiler tespit edildikten sonra anlam kazanır. Bu nedenle uygulamada daha gerçekçi muhatap, çoğu zaman güvenlik yükümlülüğünü yerine getirmediği için verinin sızmasına yol açan veri sorumlusudur. Soruşturmada veya Kurul incelemesinde verinin kaynağının belirlenmesi, bu davanın ispatını büyük ölçüde kolaylaştırır. Görevli yargı yeri de verinin kaynağına göre değişir. Kurt Konca'nın belirttiği gibi veri sorumlusu bir kamu tüzel kişisiyse zararın tazmini için idare mahkemesinde tam yargı davası açılır (Kurt Konca, s. 485), özel hukuk kişisiyse dava adli yargıda görülür. Veri sorumlusu ile mağdur arasındaki ilişki bir tüketici, iş veya ticari ilişkiyse ihtisas mahkemelerinin görevi gündeme gelebilir (Kurt Konca, s. 478).

BÖLÜM VII

Bilgileri Panelde Görünen Kişi Ne Yapmalıdır?

Bilgilerin sorgu panelinde görünmesi kişiyi hiçbir sorumluluk altına sokmaz, ancak kendiliğinden de sona ermez. Panel kapanmadıkça ve faillere ulaşılmadıkça veri dolaşımda kalmaya devam eder. Etkili sonuç, delillerin özgün halleriyle korunması, suç duyurusunda panelin ödeme ve dağıtım izlerinin gösterilmesi, verinin kaynağına ilişkin KVKK başvurusunun süresinde yapılması ve kötüye kullanım riskine karşı hesapların güvence altına alınmasıyla elde edilir. TCK m. 136 kapsamındaki suç resen soruşturulduğu için mağdurun başvurusu soruşturmayı başlatan değil yönlendiren bir işlev görür. Kişisel veri suçları ve siber güvenlik suçları bakımından deneyimli bir bilişim avukatı veya bilişim suçları avukatı ile çalışmak, özellikle verinin kaynağının tespiti ve tazminat davasının hazırlanması aşamalarında sürecin doğru kurulmasını sağlar.

EK

Kaynaklar

1. Yargıtay 12. Ceza Dairesi, 12.05.2025, E. 2025/449, K. 2025/4296.
2. Yargıtay 12. Ceza Dairesi, 23.06.2025, E. 2025/361, K. 2025/5540.
3. Yargıtay 12. Ceza Dairesi, 05.01.2026, E. 2025/2253, K. 2026/27.
4. Yargıtay 12. Ceza Dairesi, 07.04.2026, E. 2025/8484, K. 2026/3419.
5. Yargıtay 12. Ceza Dairesi, 13.04.2026, E. 2024/1437, K. 2026/3678.
6. Orhan Gazi Yaşar, Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK M. 136/1-2), Yüksek Lisans Tezi, Ankara Sosyal Bilimler Üniversitesi, 2023, Tez No. 793622, Ulusal Tez Merkezi.
7. Fatma Dilan Topuz, Kişisel Verilerin Kaydedilmesi, Başkasına Verilmesi veya Ele Geçirilmesi (TCK m. 135-137), Yüksek Lisans Tezi, Marmara Üniversitesi, 2017, Tez No. 492912, Ulusal Tez Merkezi.
8. Ayşenur Yıldız, KVKK ve GDPR Işığında Veri İhlali ve Sonuçları, Yüksek Lisans Tezi, MEF Üniversitesi, 2024, Tez No. 906885, Ulusal Tez Merkezi.
9. Hasan Sınar, Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK md. 136), Kişisel Verileri Koruma Dergisi, C. 2, S. 1, 2020, s. 33-62.
10. Duygu Tüzün Karakoçak, Gizli Sosyal Medya Profiline Erişim Sağlayan Uygulamaların Ceza Hukuku Bakımından Değerlendirilmesi, Periodicum Iuris, 2026.

11. Mehmet Bedii Kaya, Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law, Annales de la Faculté de Droit d'Istanbul, C. 70, 2021, s. 195 vd.
12. Nesibe Kurt Konca, Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme, İnönü Üniversitesi Hukuk Fakültesi Dergisi, C. 13, S. 2, 2022, s. 476-490.

Çevrimiçi sürüm: https://burakucuncu.com.tr/sorgu-paneli-bilgilerim-cikiyor