T.C.
BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
KAMU YÖNETİMİ VE SİYASET BİLİMİ ANABİLİM DALI

TÜRK KAMU YÖNETİMİNDE DİJİTALLEŞME VE HUKUKİ BOYUTU

Dürdane ÖZKAN

YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Mustafa LAMBA

BURDUR – 2025

T.C.
BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
KAMU YÖNETİMİ VE SİYASET BİLİMİ ANABİLİM DALI

TÜRK KAMU YÖNETİMİNDE DİJİTALLEŞME VE HUKUKİ BOYUTU

Dürdane ÖZKAN

YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Mustafa LAMBA
Üye: Doç. Dr. Emre SAVUT
Üye: Dr. Öğr. Üyesi Emin HÜSEYİNOĞLU

BURDUR – 2025

T.C.

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ETİK BEYAN

Burdur Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğine göre hazırlamış olduğum,

"Türk Kamu Yönetiminde Dijitalleşme ve Hukuki Boyutu" adlı tezin hazırlanması sürecinde akademik etik ilkeleri ihlal etmediğimi taahhüt eder, tezimin kağıt ve elektronik kopyalarının Burdur Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım.

Sosyal Bilimler Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

Tezimin tamamı her yerden erişime açılabilir.

Tezim sadece Burdur Mehmet Akif Ersoy Üniversitesi yerleşkelerinde erişime açılabilir.

Tezimin 3 yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin tamamı her yerden erişime açılabilir.

Dürdane ÖZKAN

TEŞEKKÜR METNİ

Lisans eğitimim boyunca, ilk günden itibaren adım adım beni bu sürecin sonuna hazırlayan; bilgeliğiyle, insanlığıyla, cesaretiyle kendimi geliştirmemi, iyi hissetmemi ve bu işi başaracağıma inancımı teşvik eden, bu zorlu yolda iyi ki rehberim olmuş dediğim değerli hocam Prof. Dr. Mustafa LAMBA ‘ya,

Her daim yanımda olan desteğini her an her koşulda hissettiğim ve bana bu yolda yürümeme destek olan en başta benim buğünlere gelmeme destek olan annem Ayşe ŞEN ve babam Cevat ŞEN’ e daha sonra sevgili eşim Tevfik Serkan ÖZKAN ve kızlarım Ayça ÖZKAN, Ece ÖZKAN, Defne ÖZKAN ‘a sonsuz teşekkürlerimi sunarım.

Burdur, 2025

(ÖZKAN, Dürdane, Türk Kamu Yönetiminde Dijitalleşme ve Hukuki Boyutu, Yüksek Lisans Tezi, Burdur, 2025)

ÖZET

Günümüzde dijitalleşme, kamu yönetiminde etkinlik, şeffaflık ve erişilebilirliği artırırken, beraberinde bilişim suçları ve veri güvenliği gibi yeni riskleri de gündeme getirmiştir. Türkiye'de kamu hizmetlerinin dijital dönüşümü, e-Devlet uygulamaları ve bilgi teknolojilerinin yaygınlaşmasıyla hız kazanmış, kamu yönetiminde iş süreçlerinin modernizasyonu önemli bir gündem maddesi hâline gelmiştir. Dolayısıyla, dijitalleşmenin hukuki boyutunu anlamak hem kamu hizmetlerinin etkin yürütülmesi hem de vatandaş haklarının korunması açısından kritik bir öneme sahiptir.

Bu çalışmada, dijitalleşmenin hukuki boyutu, mevzuat incelemesi ve örnek yargı kararları üzerinden içerik analizi yöntemi kullanılarak ele alınmıştır. Araştırmada, Türk Ceza Kanunu'nun bilişim suçlarına ilişkin maddeleri ile Kişisel Verilerin Korunması Kanunu başta olmak üzere ilgili diğer yasal düzenlemeler değerlendirilmiştir. Özellikle Türk Ceza Kanunu'nun Topluma Karşı Suçlar başlıklı Üçüncü kısmının, Bilişim Alanında Suçlar başlıklı Onuncu Bölümünde yer alan 243 ila 246. maddeler detaylı olarak incelenmiş, içerik analizi yöntemiyle mevcut düzenlemelerin kapsamı, eksiklikleri ve uygulanabilirliği tespit edilmiştir.

Araştırmanın bulguları, mevcut mevzuatın bilişim suçlarına karşı önemli bir çerçeve sağlamakla birlikte, teknolojik gelişmeler karşısında yetersiz kaldığını göstermektedir. Yapay zeka, nesnelerin interneti ve blok zinciri gibi yeni teknolojilerle birlikte ortaya çıkan suç türleri için mevcut düzenlemelerin güncellenmesi gerekmektedir. Ayrıca, bilişim suçlarının soruşturulması ve kovuşturulmasında teknik bilgi gereksinimi, delil toplama güçlükleri ve uluslararası işbirliğinin sınırlılığı etkin mücadeleyi zorlaştırmaktadır.

Çalışma, hukuki düzenlemelerin sürekli yenilenmesi, kurumsal kapasitenin güçlendirilmesi, toplumsal bilinçlendirme ve uluslararası işbirliğinin artırılmasının önemini vurgulamaktadır. Türkiye'nin dijital dönüşüm sürecinde bilişim suçlarıyla etkili mücadele edebilmesi için bütüncül, sürdürülebilir ve hukuka uygun stratejilere ihtiyaç duyulduğu sonucuna ulaşılmıştır. Ayrıca, dijitalleşmenin kamu yönetiminde daha etkin ve hukuka uygun şekilde uygulanabilmesi için mevzuatın sürekli güncellenmesi, teknik

uzmanlık ve kurumsal altyapının güçlendirilmesi, vatandaşların bilinçlendirilmesi ve uluslararası işbirliklerinin geliştirilmesi gerekliliği sonucuna ulaşılmıştır.

Anahtar Kelimeler: Dijitalleşme, Kamu Yönetimi, Bilişim Suçları, e-Devlet, Veri Güvenliği, Kişisel Verilerin Korunması

(ÖZKAN, Dürdane, Digitalization and its Legal Dimension in Turkish Public Administration, Master's Thesis, Burdur, 2025)

ABSTRACT

Today, digitalization enhances efficiency, transparency, and accessibility in public administration, while also bringing new risks such as cybercrimes and data security concerns. The digital transformation of public services in Türkiye has accelerated with the expansion of e-Government applications and information technologies, making the modernization of administrative processes a significant agenda item. Therefore, understanding the legal dimension of digitalization is critically important for both the effective delivery of public services and the protection of citizens' rights.

In this study, the legal dimension of digitalization is examined through content analysis based on a review of relevant legislation and sample judicial decisions. The research evaluates the provisions of the Turkish Penal Code concerning cybercrimes, as well as the Law on the Protection of Personal Data and other related regulations. In particular, Articles 243 to 246 of the Tenth Section titled "Crimes in the Field of Informatics," located in the Third Part of the Code under "Crimes Against Society," are examined in detail. Through content analysis, the scope, shortcomings, and applicability of the current regulations are identified.

The findings of the study reveal that although the existing legislation provides an important framework for combating cybercrimes, it remains insufficient in the face of technological advancements. With emerging technologies such as artificial intelligence, the Internet of Things, and blockchain, new types of crimes have appeared, requiring updates to current regulations. Additionally, challenges such as the need for technical expertise, difficulties in collecting evidence, and limited international cooperation hinder effective investigation and prosecution of cybercrimes.

The study emphasizes the importance of continuously updating legal regulations, strengthening institutional capacity, raising public awareness, and enhancing international cooperation. It concludes that Türkiye needs holistic, sustainable, and legally compliant strategies to effectively combat cybercrimes during its digital transformation process. Furthermore, it finds that for digitalization to be implemented more effectively and lawfully in public administration, continuous legislative updates,

strengthened technical expertise and institutional infrastructure, increased public awareness, and improved international collaboration are necessary.

Keywords: Digitalization, Public Administration, Cybercrimes, e-Government, Data Security, Personal Data Protection

İÇİNDEKİLER

KISALTMALAR VE SİMGELER

AB	:Avrupa Birliği
ABD	:Amerika Birleşik Devletleri
A.Ş.	:Anonim Şirketi
BGYS	: Bilgi Güvenliği Yönetim Sistemlerinin
BM	:Birleşmiş Milletler
BTK	:Bilgi Teknolojileri ve İletişim Kurumu
CERT	: Siber Olaylara Müdahale Merkezi
CERT-EU	: Birlik Kurumları, Organları, Ofisleri ve Ajansları için Siber Güvenlik Hizmeti
CFAA	: Computer Froud and Abuse Act
CMK	: Ceza Muhakemeleri Kanunu
COVİD-19	: Yeni Koronavirüs Hastalığı
DDO	: Dijital Dönüşüm Ofisi
DDoS	: Hizmet Engelleme Saldırıları
EGM	: Emniyet Genel Müdürlüğü
ENISA	: Avrupa Siber Güvenlik Ajansı
GDRP	: Avrupa Birliği Genel Veri Koruma Yönetmeliği
GSM	: Mobil İletişim İçin Küresel Sistem
HAGB	:Hükmün Açıklanmasının Geri Bırakılması
IDS/IPS	: Önleme Sistemleri
IoT	:Nesnelerin İnterneti
IP	:Internet Protocol Address
ITU Union)	:Uluslararası telekomünikasyon birliği (International Telecommunication
KSGM	: Kamu Siber Güvenlik Merkezi
KVKK	: Kişisel Verileri Koruma Kanunu
md.	:Kanun Maddesi
MEB	: Milli Eğitim Bakanlığı
MITM	:Man İnThe Middle (Ortadaki Adam)
OECD	: Ekonomik İşbirliği ve Kalkınma Örgütü
SSL/TLS	: Güçlü Şifreleme Protokolleri

TBMM	: Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TCK	: Türk Ceza Kanunu
TÜBİTAK	: Türkiye Bilimsel ve Teknik Araştırma Kurumu
UNODC	:Birleşmiş Milletler Suçla Mücadele Ofisi
VNP	: Virtual Private Network (Sanal Özel Ağ)
WEB	: World Wide Web
Wİ-Fİ	: Wireless Fidelity (Kablosuz Yerel Ağ)

GİRİŞ

Bu çalışma, Türkiye'de kamu yönetiminde dijitalleşme sürecinin hukuki boyutlarını detaylı bir şekilde incelemeyi amaçlamaktadır. Dijitalleşmenin kamu hizmetlerinin etkinlik, erişilebilirlik ve şeffaflık açısından önemli kazanımlar sağladığı; vatandaş-devlet ilişkilerinde bürokrasinin azalmasına ve işlem hızının artmasına katkıda bulunduğu tespit edilmiştir. Bununla birlikte, dijital dönüşüm sürecinin beraberinde getirdiği bilişim suçları, kamu kurumlarının bilgi güvenliğini tehdit eden ve toplumun dijital altyapısını zayıflatan ciddi risk unsurları olarak ortaya çıkmaktadır. Çalışmada, bilişim suçlarının tanımı, gelişimi, türleri ve etkileri sistematik olarak analiz edilmiş; Türk Ceza Kanunu (TCK) ve Kişisel Verilerin Korunması Kanunu (KVKK) başta olmak üzere ilgili mevzuatın bilişim suçlarıyla mücadeledeki rolü değerlendirilmiştir.

Mevcut hukuki düzenlemelerin, teknolojinin hızla değişen dinamiklerine ve bilişim suçlarının karmaşık yapısına yeterince cevap veremediği, özellikle yapay zeka, blok zinciri ve nesnelerin interneti gibi yeni teknolojilerin ortaya çıkardığı suç türlerine karşı mevzuatın güncellenmesinin zorunlu olduğu ortaya konmuştur. Ayrıca, bilişim suçlarının soruşturulması ve kovuşturulmasında teknik bilgi eksikliği, delil toplamadaki güçlükler ve uluslararası işbirliği mekanizmalarının zayıf olması gibi uygulamadaki sorunlar, etkin mücadeleyi sınırlamaktadır.

Bu bağlamda, çalışmada Türkiye Büyük Millet Meclisi bünyesinde Bilişim Hukuku Sürekli İzleme Komisyonu kurulmasının önemi vurgulanmış; mevzuatın güncel tutulması ve teknolojik gelişmelere hızlı adaptasyonun sağlanması önerilmiştir. Kurumsal kapasitenin artırılması, bilişim suçlarıyla mücadele eden birimlerin güçlendirilmesi, personelin düzenli ve kapsamlı eğitimlerle donatılması gerekliliği de ortaya çıkmıştır. Ayrıca, kamu ve özel sektör arasında bilgi paylaşımı ve koordinasyonun sağlanması, kritik altyapıların korunmasına yönelik stratejik işbirliklerinin geliştirilmesi önemli tedbirler arasında yer almaktadır.

Çalışmada ayrıca, adli ve kolluk personelinin bilişim suçları konusunda uzmanlaşmasının zorunluluğu belirtilmiş; Adalet Bakanlığı bünyesinde Siber Suçlar Uzmanlığı sertifika programlarının zorunlu hale getirilmesi ve bu programların düzenli güncellenmesi önerilmiştir. Toplumsal bilinçlendirme faaliyetlerinin de bilişim suçlarıyla

mücadelede etkin bir unsur olduğu; dijital okuryazarlığın artırılması, vatandaşların ve kamu çalışanlarının siber güvenlik farkındalığının yükseltilmesi için Milli Eğitim Bakanlığı ve sivil toplum kuruluşlarıyla işbirliği yapılması gerektiği ortaya konmuştur.

Uluslararası hukuk bağlamında ise Türkiye'nin, Budapeşte Sözleşmesi gibi uluslararası anlaşmalara taraf olarak ve sınır ötesi işbirliği mekanizmalarını etkin şekilde kullanarak bilişim suçlarıyla mücadelede aktif rol almasının önemi vurgulanmıştır. Ulusal mevzuatın uluslararası standartlarla uyumlu hale getirilmesi, siber suçlarla mücadelede küresel ağın önemli bir parçası olunması gerekliliği de çalışmanın sonuçları arasında yer almaktadır.

İlk bölümde, dijitalleşmenin kamu yönetiminde ortaya çıkardığı yapısal değişiklikler ele alınmıştır. Kamu hizmetlerinin etkinliği, erişilebilirliği ve şeffaflığının artması ile vatandaş-devlet ilişkilerindeki dönüşüm detaylandırılmıştır. Ayrıca dijitalleşmenin, bürokrasinin azaltılması ve kamu operasyonlarının hızlandırılması üzerindeki etkileri tartışılmıştır.

İkinci bölüm, bilişim suçlarının kavramsal çerçevesi ve Türkiye'deki gelişimi üzerine yoğunlaşmıştır. Bilişim suçlarının tanımı, türleri, kapsamı ve toplumsal etkileri kapsamlı şekilde ele alınmış; siber saldırılar, kimlik hırsızlığı, veri manipülasyonu gibi suç örnekleri açıklanmıştır. Bu bölümde, bilişim suçlarının kamu yönetimi üzerindeki riskleri ve bu suçlara karşı alınan önlemler değerlendirilmiştir.

Üçüncü bölüm, Türkiye'nin bilişim suçlarıyla mücadelede kullandığı hukuki ve kurumsal araçları incelemiştir. TCK başta olmak üzere, KVKK gibi temel mevzuat ayrıntılı şekilde analiz edilmiş; mevzuatın bilişim suçları karşısındaki etkinliği ve yetersizlikleri ortaya konmuştur. Ayrıca, hukuki düzenlemelerin güncellenmesi gerekliliği, bilişim hukuku alanında sürekli izleme mekanizmalarının kurulması önerilmiştir. Kurumsal kapasitenin artırılması, siber güvenlik uzmanlığı programlarının geliştirilmesi ve kurumlar arası iş birliği konularına değinilmiştir.

Dördüncü bölüm ise bilişim suçlarıyla mücadelede stratejik ve toplumsal boyutları ele almıştır. Toplumsal bilinçlendirme, dijital okuryazarlık eğitimleri, kamu ve özel sektör iş birliği, uluslararası hukuk ve iş birliği mekanizmalarının önemi vurgulanmıştır. Budapeşte Sözleşmesi gibi uluslararası anlaşmaların uygulanması ve sınır

ötesi iş birliğinin güçlendirilmesi gerektiği belirtilmiştir. Ayrıca, kamu yönetiminin dijital güvenlik kültürünü yaygınlaştırma ve vatandaşları bilinçlendirme rolü tartışılmıştır.

Sonuç olarak, Türkiye'de kamu yönetiminin dijitalleşme süreci, kamu hizmetlerinin verimliliğini ve vatandaş memnuniyetini artırırken, bilişim suçları ve siber güvenlik risklerini de beraberinde getirmektedir. Bu doğrultuda, bilişim suçlarıyla mücadelede hukuki, kurumsal, teknik ve toplumsal boyutları kapsayan çok katmanlı ve sürdürülebilir bir strateji geliştirilmesi elzemdir. Ancak bu şekilde, dijital dönüşüm sürecinde ortaya çıkan tehditler minimize edilebilir ve kamu yönetiminde güvenilirlik ile süreklilik sağlanabilir.

BİRİNCİ BÖLÜM

KAMU YÖNETİMİNDE DİJİTALLEŞME

1.1. Dijitalleşme Kavramı ve Kamu Yönetimine Etkileri

Dijitalleşme, günümüzde kamu yönetiminin yapısını ve işleyişini köklü biçimde dönüştüren temel süreçlerden biridir. Bu kavram, yalnızca geleneksel bilgilerin dijital ortama aktarılması anlamına gelmeyip, bilgi ve iletişim teknolojilerinin kamu kurumlarında kullanılmasıyla birlikte yönetim anlayışının, hizmet sunumunun, karar alma mekanizmalarının ve vatandaşlarla ilişkilerin yeniden şekillenmesini ifade etmektedir (Küçük, 2022: 12). Dijitalleşme, kamusal alanın daha etkin, şeffaf ve hesap verebilir hale gelmesi için önemli bir araçtır ve bu yönüyle hem teknolojik hem de sosyal bir dönüşüm sürecidir.

Dijitalleşmenin temel bileşenleri, veri işleme, bilgi paylaşımı, otomasyon, dijital hizmetlerin geliştirilmesi ve teknoloji tabanlı iletişim olarak sıralanabilir. Kamu yönetiminde dijitalleşme, bu bileşenlerin entegre edilmesiyle kamu hizmetlerinin daha hızlı, etkin ve vatandaş odaklı bir şekilde sunulmasını sağlamaktadır. Örneğin, dijital platformlar aracılığıyla devlet-vatandaş ilişkileri yeniden tanımlanmakta, bürokratik işlemler sadeleşmekte ve kamu kurumlarının işleyişinde verimlilik artmaktadır (OECD, 2023: 15).

Dijitalleşmenin kamu yönetimine etkilerini anlamak için öncelikle kavramsal çerçeveyi iyi kavramak gerekmektedir. Dijitalleşme, teknolojik yeniliklerin kamu yönetimine entegrasyonu anlamına gelmekle birlikte, beraberinde yönetimsel reformları, organizasyonel değişiklikleri ve vatandaş odaklı yaklaşımların yaygınlaşmasını da getirmektedir. Bu bağlamda dijitalleşme, sadece teknik bir süreç olmayıp, aynı zamanda kültürel ve yönetsel dönüşümü ifade eden çok boyutlu bir olgudur (Yıldırım ve Bostancı, 2022: 40).

Kamu yönetiminde dijitalleşmenin en temel etkilerinden biri, hizmet sunumundaki radikal değişimdir. Geleneksel kamu hizmetlerinde fiziksel mekâna ve yüz yüze iletişime dayalı süreçler, dijitalleşme ile birlikte çevrimiçi platformlar aracılığıyla

erişilebilir hale gelmiştir. Bu durum, vatandaşların devlet hizmetlerine erişimini kolaylaştırırken, işlem sürelerini önemli ölçüde kısaltmıştır. E-Devlet uygulamaları, dijitalleşmenin somut örnekleri olarak, vatandaşların işlemlerini zamandan ve mekândan bağımsız olarak gerçekleştirmelerine olanak sağlamaktadır (Yıldırım ve Bostancı, 2022: 45). Böylece kamu hizmetleri daha kapsayıcı, erişilebilir ve kullanıcı dostu bir yapıya kavuşmuştur.

Dijitalleşme aynı zamanda kamu kurumlarında verimlilik artışına da zemin hazırlamaktadır. Bilgi teknolojilerinin kullanımı, rutin işlerin otomatikleşmesini sağlayarak personel üzerindeki iş yükünü azaltmakta, hataları minimize etmekte ve bilgi akışını hızlandırmaktadır (Şahin, 2023: 103). Bu sayede kamu kurumları, sınırlı kaynakları daha etkin kullanarak hizmet kalitesini artırabilmektedir. Ayrıca dijital araçlar, performans yönetimi sistemlerinin gelişmesini desteklemekte, kurumların süreçlerini analiz ederek iyileştirmelerine imkân vermektedir.

Şeffaflık ve hesap verebilirlik, dijitalleşmenin kamu yönetimine sağladığı diğer önemli katkılardandır. Dijital platformlar sayesinde, kamu işlemlerine dair bilgiler daha şeffaf bir şekilde paylaşılmakta, vatandaşlar devletin faaliyetlerini daha yakından takip edebilmektedir (Küçük, 2022: 56). Bu durum, yolsuzluk ve suiistimal risklerini azaltmakta, kamu kurumlarının hesap verebilirlik mekanizmalarını güçlendirmektedir. Dolayısıyla, dijitalleşme, demokratik yönetim ilkeleri ile kamu yönetiminin etkinliğini destekleyen bir araç olarak karşımıza çıkmaktadır (Yıldız ve Kocaoğlu, 2024: 50).

Kamu yönetiminde dijitalleşmenin bir başka önemli boyutu, veri yönetimi ve karar alma süreçleridir. Büyük veri, yapay zeka ve makine öğrenimi gibi teknolojiler, kamu kurumlarının karmaşık veri setlerini analiz ederek daha isabetli kararlar almasını mümkün kılmaktadır (OECD, 2023: 22). Bu sayede politika yapıcılar, sorunları önceden tespit edebilmekte, kaynak tahsisinde ve stratejik planlamada daha etkin olabilmektedir. Özellikle acil durum yönetimi ve kriz senaryolarında dijital teknolojilerin rolü giderek artmaktadır.

Öte yandan dijitalleşmenin kamu yönetimine getirdiği avantajların yanı sıra, önemli riskler ve zorluklar da mevcuttur. Dijital uçurum, yani toplumun farklı kesimleri arasındaki dijital erişim ve kullanım eşitsizliği, kamu hizmetlerine erişimde adaletsizlikler yaratabilmektedir (OECD, 2023: 24). Bu durum, özellikle dezavantajlı

grupların kamu hizmetlerinden yeterince yararlanamaması riskini doğurmaktadır. Bu nedenle, dijitalleşmenin kapsayıcı olması için eğitim ve altyapı yatırımlarının artırılması zorunludur.

Veri güvenliği ve kişisel mahremiyetin korunması da dijitalleşmenin önemli bir boyutudur. Kamu kurumlarının topladığı ve işlediği kişisel verilerin güvenliği, vatandaşların devlet kurumlarına olan güvenini doğrudan etkileyen bir unsurdur (Eryılmaz, 2018: 80). Siber saldırılar, veri ihlalleri ve kötüye kullanım riskleri, kamu kurumlarının siber güvenlik alanında ciddi yatırımlar yapmasını zorunlu kılmaktadır. Ayrıca yasal düzenlemelerle veri koruma standartlarının belirlenmesi, bu alandaki temel gereksinimlerden biridir.

Kamu personelinin dijital dönüşüme uyumu, dijitalleşmenin başarısı açısından kritik önemdedir. Teknolojinin etkin kullanımı için personelin dijital becerilerinin artırılması, sürekli eğitim programları ve değişim yönetimi süreçlerinin etkin uygulanması gerekmektedir (Şahin, 2023: 110). Personelin teknolojiye adaptasyonu sağlanamadığında, dijitalleşmenin potansiyel faydaları tam olarak gerçekleştirilememektedir. Bu bağlamda, kamu yönetiminde insan kaynakları politikalarının da dijitalleşme stratejileriyle uyumlu hale getirilmesi önem taşımaktadır.

Türkiye'de dijitalleşme süreci, son yıllarda çeşitli reformlar ve projelerle hız kazanmıştır. 2008 yılında kurulan e-Devlet Kapısı, vatandaşların devletle elektronik ortamda etkileşimini kolaylaştıran en önemli adımlardan biri olmuştur (Küçük, 2022: 14). Bu platform, kamu hizmetlerine hızlı ve güvenli erişim sağlamanın yanı sıra, devletin şeffaflığını artırıcı bir araç olarak işlev görmektedir. Ayrıca Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin kurulması, dijitalleşme politikalarının koordinasyonu ve uygulanmasında merkezi bir rol üstlenmiştir (OECD, 2023: 25). Yerel yönetimlerde de dijital hizmetlerin yaygınlaşması, vatandaş odaklı hizmet anlayışının güçlenmesine katkıda bulunmuştur (Tutar , 2023: 30).

Dijitalleşme, kamu yönetiminde organizasyonel yapıyı da önemli ölçüde etkilemektedir. Geleneksel hiyerarşik yapıların yerini, daha esnek, yatay iletişim ve iş birliği mekanizmalarına sahip organizasyonlar almaktadır (Yıldırım, 2021: 78). Bu dönüşüm, bilgi akışını hızlandırmakta ve kurumlar arası koordinasyonu artırmaktadır. Özellikle dijital platformlar aracılığıyla kurumlar arasında veri paylaşımı kolaylaşmakta

ve iş süreçleri daha entegre hale gelmektedir (Şimşek ve Demir, 2022: 98). Ancak bu süreç, kurumsal direncin yönetilmesini ve personelin değişime uyum sağlamasını gerektirmektedir (Yıldız ve Kocaoğlu, 2024: 58).

Kamu politikalarının oluşturulmasında dijital teknolojilerin kullanımı, politika yapıcıların veri temelli kararlar almasına olanak tanımaktadır (OECD, 2023: 27). Büyük veri analitiği ve yapay zeka uygulamaları, toplum ihtiyaçlarının daha iyi anlaşılmasını ve hizmetlerin buna göre şekillendirilmesini sağlamaktadır. Özellikle sağlık, eğitim ve güvenlik alanlarında dijitalleşme, kamu hizmetlerinin etkinliğini artırmakta ve krizlere hızlı müdahale imkânı sunmaktadır (Küçük, 2022: 35). Öte yandan veri mahremiyeti ve etik sorunlar, dijitalleşme politikalarının tasarımında dikkat edilmesi gereken önemli konulardır (Eryılmaz, 2018: 87).

Vatandaşlarla devlet arasındaki ilişkiler de dijitalleşmeden önemli ölçüde etkilenmiştir. E-Devlet uygulamaları, vatandaşların devletle hızlı ve doğrudan iletişim kurmasını mümkün kılmakta, kamu hizmetlerine erişimde kolaylık sağlamaktadır (Yıldırım ve Bostancı, 2022: 47). Dijital platformlar, vatandaşların kamu karar alma süreçlerine katılımını artırmakta, demokratik yönetim ilkelerinin hayata geçirilmesini desteklemektedir (Şimşek ve Demir, 2022: 105). Ancak dijital okuryazarlık ve erişim farklılıkları, dijitalleşmenin sosyal boyutta kapsayıcılığını zorlayan faktörler olarak öne çıkmaktadır (OECD, 2023: 28).

Gelecekte, yapay zeka, nesnelerin interneti, blok zincir ve robotik otomasyon gibi teknolojilerin kamu yönetiminde daha yaygın kullanılması beklenmektedir (OECD, 2023: 30). Bu teknolojiler, kamu hizmetlerinin kişiselleştirilmesini, otomatikleştirilmesini ve daha güvenilir hale getirilmesini sağlayacaktır (Küçük, 2022: 40). Akıllı şehir uygulamaları gibi yeni yaklaşımlar, vatandaş yaşam kalitesini artırmakta ve kamu altyapılarını optimize etmektedir (Yıldırım, 2021: 85). Ancak, teknolojik gelişmelerin getirdiği etik, hukuki ve sosyal sorunların da dikkatle ele alınması gerekmektedir (Eryılmaz, 2018: 92).

Sonuç olarak, dijitalleşme kamu yönetiminde vazgeçilmez bir unsur haline gelmiş olup, yönetim süreçlerini ve hizmet sunumunu temelden değiştirmektedir. Dijitalleşmenin sunduğu fırsatlardan tam olarak yararlanmak için kapsayıcı politikalar geliştirilmesi, personel eğitimine yatırım yapılması, siber güvenlik önlemlerinin

artırılması ve vatandaşların dijital okuryazarlığının yükseltilmesi gerekmektedir. Bu kapsamda, dijitalleşme sadece teknolojik bir ilerleme değil, aynı zamanda kamu yönetiminin etkinliği, şeffaflığı ve demokratik yapısının güçlendirilmesi için stratejik bir dönüşüm süreci olarak ele alınmalıdır.

1.2. Türkiye'de Kamu Yönetiminde Dijitalleşme Süreci

Kamu yönetiminde dijitalleşme, modern devletlerin yönetim kapasitesini artırmak, hizmet kalitesini yükseltmek ve vatandaş memnuniyetini sağlamak amacıyla teknolojik altyapıların etkin kullanımı olarak tanımlanabilir. Türkiye'de dijitalleşme süreci, 2000'li yılların başından itibaren, özellikle küresel dijital dönüşüm trendleri ve ulusal stratejik planlar çerçevesinde şekillenmeye başlamıştır. Bu süreç, hem kamu kurumlarının işleyiş mekanizmalarını hem de vatandaşlarla devlet arasındaki etkileşim biçimlerini köklü bir biçimde değiştirmiştir. Türkiye'nin dijitalleşme alanındaki yolculuğu, kamu yönetiminde verimlilik, şeffaflık ve hesap verebilirlik ilkelerinin güçlendirilmesi açısından önemli bir dönüm noktası olmuştur.

Türkiye'de dijitalleşmenin kamu yönetimine entegrasyonu, 2003 yılında yayımlanan Bilgi Toplumu Stratejisi ile resmiyet kazanmıştır. Bu strateji, dijital teknolojilerin kamu hizmetlerine entegrasyonunu teşvik ederek, kamu sektöründe bilgi ve iletişim teknolojilerinin yaygınlaştırılması hedefini ortaya koymuştur (T.C. Başbakanlık, 2003: 12). Bu dönemde kamu kurumlarının altyapı yatırımları artırılmış, elektronik ortamda hizmet sunumu konusunda pilot uygulamalar başlatılmıştır. Özellikle 2008 yılında faaliyete geçen e-Devlet Kapısı (www.turkiye.gov.tr), Türkiye'nin dijitalleşme sürecinde önemli bir kilometre taşı olmuştur. Bu platform, vatandaşların devletle olan iletişimini kolaylaştırmakta, kamu hizmetlerine erişimde zaman ve mekân bağımsızlığı sağlamaktadır (Küçük ve Şimşek, 2020: 113).

Dijitalleşme süreci yalnızca hizmet sunumu ile sınırlı kalmamış, kamu kurumlarının yapısal dönüşümünü de beraberinde getirmiştir. 2018 yılında kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, dijitalleşme politikalarının koordinasyonu ve stratejik yönetimi açısından kritik bir rol üstlenmiştir. Bu ofis, kamu kurumlarının dijital altyapılarının güçlendirilmesi, siber güvenlik önlemlerinin artırılması ve dijital yetkinliklerin geliştirilmesi için politikalar üretmektedir. Kurumsal dijitalleşme ile

bürokratik işlemler sadeleştirilmiş, süreçler hızlanmış ve kaynakların etkin kullanımı sağlanmıştır (Özdemir, 2022: 79).

Dijitalleşmenin yasal ve hukuki altyapısı da süreçle paralel olarak gelişmiştir. 2007 senesinde kabul edilen 5070 sayılı Elektronik İmza Kanunu, dijital belgelerin güvenilirliğini ve hukuki geçerliliğini temin etmiştir. 2016 senesinde yürürlüğe giren KVKK ise vatandaşların kişisel verilerinin dijital ortamlarda korunmasına yönelik kapsamlı düzenlemeler getirmiştir. Bu yasal düzenlemeler, dijitalleşme sürecinde güvenlik ve gizlilik kaygılarını azaltarak vatandaşların dijital hizmetlere olan güvenini artırmıştır.

Türkiye'de dijital kamu hizmetlerinin geliştirilmesinde vatandaş odaklılık temel prensiplerden biridir. E-Devlet Kapısı, vatandaşların devletle olan etkileşimini kolaylaştırırken, kamu hizmetlerinin şeffaflığı ve hesap verebilirliği artırmaktadır (Yıldırım, 2022: 91). Dijital platformlar üzerinden sunulan hizmetler, vatandaşların devlet kurumlarına gitme ihtiyacını azaltmakta, işlem sürelerini kısaltmakta ve bürokratik engelleri azaltmaktadır. Bununla birlikte, dijitalleşmenin toplumun her kesimine eşit erişim sağlayabilmesi için dijital uçurumun kapatılması büyük önem taşımaktadır. Bu amaçla kırsal bölgelerde altyapı yatırımları artırılmış, dijital okuryazarlık programları hayata geçirilmiş ve mobil teknolojiler kamu hizmetlerine entegre edilmiştir (Kaya ve Aydın, 2021: 61).

Sosyoekonomik açıdan bakıldığında, dijitalleşme kamu sektöründe verimliliği artırmış, işlem maliyetlerini düşürmüş ve iş süreçlerini optimize etmiştir (Özdemir ve Çelik, 2023: 112). Ayrıca dijital becerilere sahip insan kaynağının gelişimi, Türkiye ekonomisinin genel dijital dönüşümüne katkıda bulunmuştur. Kamu yönetimindeki dijitalleşme, kriz dönemlerinde de esnek ve etkin hizmet sunumu sağlamış; örneğin COVID-19 pandemisi sırasında dijital kamu hizmetleri vatandaşların sağlık, eğitim ve sosyal yardım hizmetlerine kesintisiz erişimini mümkün kılmıştır (Yıldırım ve Kaya, 2023: 56).

Geleceğe yönelik olarak Türkiye'nin dijitalleşme stratejilerinde yapay zeka, büyük veri, nesnelerin interneti (IoT) ve blokzincir gibi ileri teknolojilerin entegrasyonu öncelikli alanlar olarak belirlenmiştir. Bu teknolojiler, kamu hizmetlerinin kişiselleştirilmesi, süreçlerin otomatikleştirilmesi ve veri temelli karar alma

mekanizmalarının güçlendirilmesini sağlayacaktır. Ancak dijitalleşmenin sürdürülebilirliği için siber güvenlik risklerinin etkin yönetimi, etik ve hukuki sorunların çözümü ve kapsayıcı dijital politikaların uygulanması gerekmektedir (Kaya, 2022: 102).

Sonuç olarak, Türkiye'de kamu yönetiminde dijitalleşme süreci, teknolojik gelişmelerle paralel ilerleyen, hukuki ve kurumsal altyapılarla desteklenen kapsamlı bir dönüşüm hareketidir. Bu süreç, kamu hizmetlerinin kalitesini artırmakla kalmayıp, vatandaşların devletle ilişkisini daha demokratik, şeffaf ve erişilebilir hale getirmiştir. Dijitalleşmenin önündeki engellerin aşılması ve teknolojik gelişmelerin etkin kullanımı ile Türkiye'nin kamu yönetiminde dijital dönüşüm hedeflerine ulaşması mümkün görünmektedir.

Türkiye'de kamu yönetiminde dijitalleşme sürecinin başarısı, sadece teknoloji altyapısına yapılan yatırımlarla sınırlı kalmamış, aynı zamanda insan kaynağı ve kurum kültüründe meydana gelen dönüşümle de yakından ilişkilidir. Kamu kurumlarında görev yapan personelin dijital yetkinliklerinin artırılması için kapsamlı eğitim programları düzenlenmiş, dijital okuryazarlık projeleri hayata geçirilmiştir. Bu doğrultuda, 2019 yılında başlatılan Dijital Okuryazarlık Seferberliği, kamu çalışanlarının yanı sıra vatandaşların da dijital hizmetlere erişimini kolaylaştırmayı hedeflemiştir. Bu programlar, kamu yönetiminde dijital dönüşümün sürdürülebilirliği açısından hayati önem taşımaktadır.

Dijitalleşmenin yaygınlaşmasıyla birlikte, kamu hizmetlerinde inovasyonun artırılması için çeşitli projeler geliştirilmiştir. Örneğin, Akıllı Şehir uygulamaları kapsamında İstanbul, Ankara ve İzmir gibi büyük şehirlerde trafik yönetiminden enerji tüketimine kadar pek çok alanda dijital çözümler uygulanmaya başlanmıştır (Tutar ve Kaya, 2023: 37). Bu uygulamalar, yerel yönetimlerin etkinliğini artırmakla kalmamış, aynı zamanda vatandaşların yaşam kalitesini de olumlu yönde etkilemiştir. Böylece, dijitalleşme sadece merkezi yönetimde değil, yerel yönetimlerde de önemli bir dönüşüm aracı olmuştur.

Türkiye'de dijitalleşme sürecinin önemli bir diğer boyutu da vatandaş katılımının artırılmasıdır. Dijital platformlar, vatandaşların kamu politikalarına ve karar alma süreçlerine daha aktif katılımını teşvik etmektedir. E-Devlet Kapısı üzerinde vatandaşların görüş, öneri ve şikayetlerini iletebileceği interaktif modüller geliştirilmiş,

bunun yanı sıra sosyal medya ve mobil uygulamalar aracılığıyla da geri bildirim mekanizmaları güçlendirilmiştir (Kaya ve Aydın, 2021: 63). Bu gelişmeler, kamu yönetiminin daha şeffaf ve hesap verebilir hale gelmesine katkı sağlamaktadır.

Hukuki açıdan değerlendirildiğinde, dijitalleşme süreci beraberinde yeni zorluklar ve sorumluluklar getirmiştir. Özellikle veri güvenliği ve kişisel verilerin korunması konuları, kamu kurumlarının öncelikli gündem maddeleri arasında yer almaktadır. KVKK' nın uygulanması ile veri ihlallerinin önüne geçilmeye çalışılırken, siber güvenlik alanında da kapsamlı yatırımlar yapılmaktadır (Özdemir, 2022: 83). Kamu kurumları, siber saldırılara karşı kritik altyapılarını korumak için hem teknolojik hem de idari tedbirler almaktadır. Bununla birlikte, dijitalleşme sürecinde ortaya çıkan etik ve hukuki sorunların çözümü için mevzuatın sürekli güncellenmesi gerekmektedir.

Sosyoekonomik etkiler açısından bakıldığında, dijitalleşme Türkiye'de kamu sektöründe maliyet etkinliği sağlamış, iş süreçlerini hızlandırmış ve vatandaş memnuniyetini artırmıştır (Yıldırım, S., ve Özer, M. A., 2022: 221-250). Kamu hizmetlerinin dijital platformlar üzerinden sunulması, işlem sürelerinin azalması ve bürokratik engellerin ortadan kalkması ile vatandaşların devletle olan ilişkisi daha etkin hale gelmiştir (Yıldırım, 2022: 93). Özellikle genç nüfusun dijital hizmetlere hızlı adapte olması, dijitalleşmenin yaygınlaşmasını kolaylaştırmıştır. Ancak, dijital uçurumun kapatılması için kırsal kesimlerde ve dezavantajlı gruplarda altyapı yatırımlarının artırılması halen önemli bir ihtiyaçtır.

Pandemi dönemi, dijitalleşmenin önemini ve gerekliliğini bir kez daha gözler önüne sermiştir. COVID-19 salgını sürecinde, kamu hizmetlerinin dijital platformlar üzerinden kesintisiz sunulması, sosyal mesafe kurallarına uyum sağlanması ve vatandaşların sağlık, eğitim ve sosyal destek hizmetlerine erişiminin devam ettirilmesi sağlanmıştır (Yıldırım ve Kaya, 2023: 59). Bu dönem, dijitalleşmenin kamu yönetimi için sadece bir seçenek değil, zorunluluk olduğu gerçeğini ortaya koymuştur. Pandeminin ardından da dijital dönüşüm hız kesmeden devam etmiş ve yeni teknolojilerin entegrasyonu hızlandırılmıştır.

Türkiye'nin dijitalleşme yolculuğunda, ileri teknolojilerin kamu yönetimine entegrasyonu önemli bir yer tutmaktadır. Yapay zeka uygulamaları, kamu hizmetlerinin otomasyonu ve veri analitiği alanında kullanılmaya başlanmıştır. Büyük veri analizi

sayesinde, kamu politikalarının daha veri odaklı ve etkin biçimde tasarlanması mümkün hale gelmiştir. Nesnelerin interneti (IoT) ise özellikle akıllı şehir uygulamalarında yoğun olarak kullanılmakta, trafik, enerji, atık yönetimi gibi alanlarda gerçek zamanlı veri toplanmasını ve analizini sağlamaktadır. Blokzincir teknolojileri ise kamu işlemlerinde şeffaflık ve güvenilirlik sağlamak amacıyla pilot projelerde denenmektedir.

Öte yandan, dijitalleşmenin getirdiği sosyal ve etik sorunlar da dikkatle ele alınmalıdır. Dijital ortamda veri gizliliği, dijital haklar, ayrımcılık ve erişim eşitsizliği gibi konular, kamu yönetiminde politikaların ve uygulamaların şekillenmesinde önemli bir rol oynamaktadır (Kaya, 2022: 105). Bu nedenle, dijitalleşme sürecinde sadece teknolojik altyapının güçlendirilmesi değil, aynı zamanda sosyal politikaların da uyumlu şekilde geliştirilmesi gerekmektedir.

Sonuç olarak, Türkiye'de kamu yönetiminde dijitalleşme süreci kapsamlı ve çok boyutlu bir dönüşüm hareketi olarak ortaya çıkmaktadır. Bu süreç, teknolojik gelişmelerle birlikte hukuki, kurumsal, sosyal ve ekonomik alanlarda eşzamanlı değişimleri gerektirmektedir. Kamu hizmetlerinin kalitesini artırmak, vatandaşların devlete olan güvenini pekiştirmek ve yönetim süreçlerini etkinleştirmek için dijitalleşme stratejilerinin uygulanması kritik önemdedir. Türkiye, dijitalleşme yolculuğunda ilerlerken, karşılaşılan engelleri aşmak ve teknolojik yenilikleri etkin kullanmak suretiyle modern, şeffaf ve vatandaş odaklı bir kamu yönetimi modeli inşa etmeye devam etmektedir.

1.3. E-Devlet ve Dijital Kamu Hizmetleri

E-Devlet kavramı, kamu hizmetlerinin bilgi ve iletişim teknolojileri aracılığıyla sunulması anlamına gelmekte olup, modern kamu yönetiminin dijital dönüşümünün temel yapı taşlarından biridir. Dijital kamu hizmetleri ise, devletin vatandaşlara, işletmelere ve diğer kurumlara elektronik ortamda sağladığı hizmetlerin bütününü ifade eder. E-Devlet uygulamaları, kamu sektöründe etkinliği, şeffaflığı ve erişilebilirliği artırarak devlet ile vatandaşlar arasındaki etkileşim biçimini köklü biçimde değiştirmiştir. Türkiye'de e-Devlet uygulamaları, 2000'li yılların başından itibaren önemli ilerlemeler kaydetmiş ve günümüzde dijital kamu hizmetleri alanında bölgesel bir örnek ülke konumuna yükselmiştir.

E-Devletin tarihçesi, bilgi toplumuna geçiş sürecindeki teknolojik gelişmelerle paralel olarak şekillenmiştir. Dünya genelinde 1990'ların sonu ve 2000'lerin başında

internet teknolojilerinin yaygınlaşmasıyla devletler, kamu hizmetlerini dijital ortama taşıma çalışmalarına hız vermiştir. Bu bağlamda e-Devlet, sadece bir teknoloji kullanımı değil, aynı zamanda kamu yönetiminde süreçlerin yeniden yapılandırılması, kurumsal kapasitenin artırılması ve vatandaş odaklı hizmet anlayışının geliştirilmesi anlamına gelir (Heeks, 2006: 146). E-Devlet uygulamalarının başarısı, ülkelerin teknolojik altyapı gücü, yasal düzenlemeler, kurumsal yapı ve insan kaynağı kalitesi gibi çok boyutlu faktörlere bağlıdır.

Türkiye'de e-Devlet uygulamalarının gelişimi, 2003 yılında yayımlanan Bilgi Toplumu Stratejisi ile hız kazanmıştır. Bu stratejiyle kamu kurumlarının dijitalleşmesi hedeflenmiş, bilgi ve iletişim teknolojileri altyapılarının yaygınlaştırılması, dijital okuryazarlığın artırılması ve e-Devlet hizmetlerinin vatandaşlara etkin biçimde sunulması amaçlanmıştır (T.C. Başbakanlık, 2003: 25). 2008 yılında kurulan e-Devlet Kapısı (www.turkiye.gov.tr) ise Türkiye'nin dijital kamu hizmetlerinde merkezi platformu olmuştur. Bu platform üzerinden yüzlerce kamu hizmeti elektronik ortamda sunulmakta, vatandaşlar ve işletmeler işlemlerini hızlı ve güvenli bir şekilde gerçekleştirebilmektedir (Küçük ve Şimşek, 2020: 115).

Dijital kamu hizmetlerinin kapsamı oldukça geniştir. Kimlik doğrulama, sosyal güvenlik, vergi işlemleri, adli işlemler, eğitim, sağlık ve belediye hizmetleri gibi farklı alanlarda dijital uygulamalar geliştirilmiştir. Özellikle mobil teknolojilerin yaygınlaşmasıyla birlikte e-Devlet hizmetlerine erişim kolaylaşmış ve vatandaşların devletle etkileşiminde önemli bir artış yaşanmıştır (Yıldırım, 2022: 88). E-Devlet platformları, sadece bilgi sağlamakla kalmayıp, aynı zamanda vatandaşların resmi işlemlerini tamamlayabildikleri interaktif araçlar olarak da işlev görmektedir.

E-Devletin vatandaşlara sağladığı temel avantajlardan biri, işlem sürelerinin kısalması ve bürokratik engellerin azaltılmasıdır. Geleneksel kamu hizmetlerinde fiziksel evrak takibi, kurumlar arası koordinasyon eksikliği ve uzun bekleme süreleri önemli sorunlar teşkil etmekteydi. Dijitalleşmeyle birlikte bu sorunlar büyük ölçüde giderilmiş, süreçlerin şeffaflığı ve izlenebilirliği artırılmıştır (Özdemir ve Çelik, 2023: 110). Böylece hem vatandaşların memnuniyeti yükselmiş hem de kamu kurumlarının operasyonel verimliliği artmıştır.

E-Devlet hizmetlerinin yaygınlaşması, aynı zamanda kamu yönetiminde şeffaflık ve hesap verebilirlik ilkelerinin güçlenmesine katkı sağlamıştır. Dijital platformlar üzerinden sunulan hizmetlerde işlemler kayıt altına alınmakta, vatandaşların talepleri ve geri bildirimleri kolayca takip edilmektedir (Kaya ve Aydın, 2021: 65). Bu durum, yolsuzluk ve usulsüzlüklerin azalmasına, kamu kaynaklarının daha etkin kullanılmasına olanak tanımaktadır. Ayrıca, e-Devlet uygulamaları kamu politikalarının tasarımında vatandaş katılımını artırmakta, demokratik süreçlerin daha kapsayıcı hale gelmesini desteklemektedir.

Bununla birlikte, Türkiye'de e-Devlet ve dijital kamu hizmetlerinin yaygınlaşması bazı zorlukları da beraberinde getirmiştir. Dijital uçurum, yani teknolojik altyapıya ve dijital hizmetlere erişimde yaşanan eşitsizlikler, önemli bir engel olarak karşımıza çıkmaktadır. Özellikle kırsal bölgelerde internet erişimi ve dijital okuryazarlık seviyesinin düşük olması, dijital kamu hizmetlerinden tam fayda sağlanmasını sınırlamaktadır (Kaya, 2022: 99). Bu nedenle devlet, dijital altyapı yatırımlarını artırmak ve dezavantajlı gruplara yönelik eğitim programları düzenlemek zorundadır.

Siber güvenlik ve veri gizliliği de e-Devlet uygulamalarının sürdürülebilirliği için kritik önemdedir. Kamu kurumları, vatandaşların kişisel verilerini korumak ve dijital hizmetlerin güvenliğini sağlamak amacıyla teknolojik ve idari önlemler almakta; bu kapsamda KVKK gibi yasal düzenlemeler uygulamaya konmuştur (Özdemir, 2022: 82). Ancak teknolojinin hızla gelişmesi, siber tehditlerin de karmaşıklaşmasına yol açmakta, bu alanda sürekli güncellenen politikalar ve yatırımlar gerekmektedir.

Türkiye'nin e-Devlet vizyonu, gelecekte dijital kamu hizmetlerinin daha da çeşitlendirilmesi, yapay zeka, büyük veri ve nesnelerin interneti gibi ileri teknolojilerin entegrasyonu üzerine odaklanmaktadır. Bu teknolojiler, kamu hizmetlerinin kişiselleştirilmesi, otomatikleştirilmesi ve daha etkin yönetilmesini mümkün kılacaktır. Ayrıca dijital vatandaşlık kavramı çerçevesinde, vatandaşların dijital hak ve sorumluluklarının geliştirilmesi, e-Devlet uygulamalarının başarısında belirleyici olacaktır.

Sonuç olarak, Türkiye'de e-Devlet ve dijital kamu hizmetleri, kamu yönetiminin etkinliğini, şeffaflığını ve vatandaş memnuniyetini artıran önemli araçlardır. Bu süreç, teknolojik altyapıların güçlendirilmesi, hukuki düzenlemelerin tamamlanması ve insan

kaynağının dijital becerilerle donatılmasıyla desteklenmektedir. Karşılaşılan zorluklara rağmen, Türkiye dijital kamu hizmetleri alanında önemli ilerlemeler kaydetmiş ve önümüzdeki yıllarda bu alandaki gelişmelerin artarak devam etmesi beklenmektedir.

Türkiye'de e-Devlet uygulamalarının yaygınlaşmasında kamu kurumlarının koordinasyonu ve stratejik planlamanın önemi büyüktür. Bu bağlamda, Dijital Dönüşüm Ofisi'nin kurulması, e-Devlet projelerinin entegrasyonu ve sürdürülebilirliği açısından kritik bir dönüm noktası olmuştur. Kurumlar arası veri paylaşımı ve süreçlerin dijitalleşmesi, bürokrasiyi azaltırken, işlemlerde hız ve doğruluğu artırmaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019: 33). Ayrıca, bu yapısal dönüşüm, kamu yönetiminin karar alma mekanizmalarında veri odaklı politikaların geliştirilmesini desteklemektedir.

E-Devlet platformlarının vatandaş odaklı tasarımı, hizmetlerin kullanıcı dostu ve erişilebilir olmasını gerektirmektedir. Türkiye'de dijital kamu hizmetleri, erişilebilirlik ve kullanılabilirlik standartları göz önünde bulundurularak geliştirilmektedir. Özellikle engelli bireyler için tasarlanan uygulamalar ve çok dilli hizmet seçenekleri, kapsayıcı kamu hizmeti anlayışının göstergesidir (Yıldırım ve Kaya, 2023: 55). Bu durum, demokratik katılımın güçlendirilmesi ve toplumsal eşitlik açısından da önem taşımaktadır.

Türkiye'de e-Devlet hizmetlerine olan talebin artması, kamu kurumlarını sürekli olarak yeni teknolojik çözümler aramaya yönlendirmektedir. Bulut bilişim, yapay zeka destekli chatbotlar ve otomatik doküman işleme sistemleri, kamu hizmetlerinin kalitesini artıran yenilikçi araçlardır. Örneğin, bazı belediyelerde yapay zeka tabanlı çağrı merkezleri vatandaşların taleplerine 7/24 yanıt verebilmekte ve işlem süreçlerini hızlandırmaktadır (Tutar ve Kaya, 2023: 37). Bu tür uygulamalar, kamu yönetiminde dijitalleşmenin somut örnekleri olarak öne çıkmaktadır.

E-Devletin yaygınlaşması ile birlikte dijital hizmetlerin kullanım oranları ve vatandaşların memnuniyeti üzerine yapılan araştırmalar da artmaktadır. Türkiye'de yapılan çeşitli saha çalışmaları, e-Devlet hizmetlerinden yararlanan vatandaşların genellikle işlem kolaylığı ve zaman tasarrufu açısından olumlu geri bildirimlerde bulunduğunu ortaya koymaktadır (Küçük ve Şimşek, 2020: 120). Ancak, bazı kullanıcılar halen dijital okuryazarlık eksikliği ve teknik sorunlar nedeniyle hizmetlerden tam olarak

faydalanamamaktadır. Bu nedenle, kamu kurumlarının eğitim ve destek faaliyetlerini artırması önemlidir.

E-Devlet uygulamalarının finansal boyutu da dikkate alınmalıdır. Dijitalleşme yatırımları başlangıçta yüksek maliyetler gerektirse de, uzun vadede kamu kaynaklarının etkin kullanımı ve işlem maliyetlerinin düşürülmesi açısından ekonomik faydalar sağlamaktadır (Özdemir ve Çelik, 2023: 117). Ayrıca, dijital hizmetlerin yaygınlaşması ile fiziksel evrak ve bürokratik işlemler azaldığı için çevresel sürdürülebilirliğe de katkı sağlanmaktadır.

Türkiye'nin e-Devlet stratejileri, sadece hizmet sunumuyla sınırlı kalmayıp aynı zamanda vatandaşların dijital katılımını artırmaya da yöneliktir. E-Demokrasi uygulamaları, dijital platformlar üzerinden vatandaşların kamu politikalarına katkıda bulunmasını mümkün kılmaktadır. Örneğin, bazı belediyeler ve bakanlıklar halkın görüşlerini almak üzere online anketler ve geri bildirim mekanizmaları kullanmaktadır (Yıldırım, 2022: 92). Bu yöntemler, kamu yönetiminin şeffaflığı ve hesap verebilirliğini desteklemektedir.

Dijital kamu hizmetlerinde karşılaşılan önemli bir diğer zorluk ise siber güvenlik riskleridir. Özellikle kişisel verilerin korunması, devletin güvenilirliğini doğrudan etkileyen bir faktör olarak öne çıkmaktadır. Türkiye'de KVKK ile vatandaşların veri güvenliği sağlanmaya çalışılmakta, ancak siber saldırılar ve veri ihlalleri riskini tamamen ortadan kaldırmak zordur. Bu nedenle, kamu kurumları ileri düzey güvenlik teknolojilerini kullanmakta ve sürekli güncellenen güvenlik politikaları uygulamaktadır.

Son yıllarda COVID-19 pandemisi, dijital kamu hizmetlerinin önemini ve kullanımını artıran önemli bir faktör olmuştur. Pandemi sürecinde sosyal mesafe kurallarının uygulanması ve fiziksel işlemlerin kısıtlanması, vatandaşları e-Devlet hizmetlerine yönlendirmiştir (Yıldırım ve Kaya, 2023: 60). Bu dönemde, sağlık hizmetlerinden sosyal destek programlarına kadar pek çok hizmet dijital platformlar üzerinden erişilebilir hale gelmiştir. Pandeminin ardından da dijitalleşmenin önemi ve yatırımlar artarak devam etmiştir.

Türkiye'nin e-Devlet ve dijital kamu hizmetlerinde ilerleyişi, uluslararası karşılaştırmalarda da olumlu bir performans sergilemektedir. Birleşmiş Milletler E-Devlet Endeksi'nde Türkiye, gelişmekte olan ülkeler arasında üst sıralarda yer almakta

ve dijital kamu hizmetleri kalitesini artırma yönünde önemli adımlar atmaktadır (UN E-Government Survey, 2022: 45). Bu başarı, stratejik planlama, yasal düzenlemeler, altyapı yatırımları ve insan kaynağı gelişimine yapılan katkıların bir sonucudur (Köse ve Yılmaz, 2021: 32).

Ancak Türkiye'nin e-Devlet hizmetlerini daha ileriye taşıması için sürekli inovasyon, dijital okuryazarlığın artırılması, kırsal ve dezavantajlı bölgelerde internet erişiminin iyileştirilmesi ve kullanıcı deneyiminin geliştirilmesi gerekmektedir. Bu hedeflere ulaşmak için kamu, özel sektör ve sivil toplum iş birliği kritik önemdedir. Dijital dönüşüm, sadece teknolojik bir süreç değil, aynı zamanda sosyal ve kültürel dönüşümü de gerektiren kapsamlı bir değişimdir (Aydın, 2019: 18).

Özetle, Türkiye'de e-Devlet ve dijital kamu hizmetleri, kamu yönetiminin modernizasyonunda merkezi bir rol oynamaktadır. Teknolojik gelişmelerin entegrasyonu, vatandaş odaklı hizmet anlayışı ve hukuki altyapının güçlendirilmesi sayesinde dijitalleşme süreci devam etmekte ve kamu hizmetlerinin kalitesi giderek yükselmektedir. Bu süreçte karşılaşılan zorlukların aşılması ve sürdürülebilir bir dijital ekosistemin oluşturulması, Türkiye'nin bilgi toplumuna dönüşümünü hızlandıracaktır.

1.4. Dijitalleşmenin Kamu Yönetiminde Verimlilik, Şeffaflık Ve Hesap Verebilirliğe Katkısı

Kamu yönetimi, toplumun ihtiyaçlarını karşılamak üzere düzenlenmiş devlet hizmetlerinin planlanması, organize edilmesi ve yürütülmesini kapsayan karmaşık bir süreçtir. Son yıllarda bilgi ve iletişim teknolojilerindeki hızlı gelişmelerle birlikte kamu yönetiminde dijitalleşme, temel bir dönüşüm aracı haline gelmiştir. Dijitalleşme, yalnızca teknolojik altyapının yenilenmesi anlamına gelmemekte, aynı zamanda kamu kurumlarının iş süreçlerinin iyileştirilmesi, vatandaşlarla etkileşimlerin daha etkin hale getirilmesi ve yönetişim mekanizmalarının şeffaflaşması gibi çok boyutlu bir değişimi ifade etmektedir (Heeks, 2006: 159). Bu bağlamda, dijitalleşmenin kamu yönetiminde verimlilik, şeffaflık ve hesap verebilirlik ilkelerine sağladığı katkılar, hem teorik hem de uygulamalı açıdan büyük önem taşımaktadır.

Geleneksel kamu bürokrasisinde sıkça karşılaşılan uzun işlem süreleri, yoğun evrak akışı ve kurumlar arası koordinasyon eksiklikleri, dijital uygulamaların yaygınlaşmasıyla birlikte önemli ölçüde azalmaya başlamıştır. Elektronik belge yönetim

sistemleri (EBYS), iş süreçlerinin otomasyona dayalı olarak yeniden tasarlanmasına imkân tanımakta; böylece işlem süreleri kısalırken hata olasılığı düşmekte ve kurumsal kaynakların daha etkin kullanılmasına katkı sağlanmaktadır.

Nitekim EBYS kullanımının kamu kurumlarında iş akışının sadeleşmesi, belge güvenliğinin artması ve işlem hızının yükselmesi gibi sonuçlar doğurduğunu belirtmektedir (Kutlutürk, L. ve Özdemirci, 2023: 214–216). Benzer şekilde elektronik kayıt ve belge yönetim sistemlerinin kurumsal verimlilik üzerinde doğrudan olumlu etkiler yarattığını ve kamuda operasyonel yükü azalttığını ifade etmektedir (Demirtel ve Gökkurt Demirtel, 2014: 89).

Bu çerçevede, Türkiye'de e-Devlet Kapısı gibi merkezi dijital hizmet platformları, çok sayıda işlemin elektronik ortamda hızlı ve güvenli biçimde gerçekleştirilmesini sağlayarak verimlilikte somut kazanımlar elde edilmesini mümkün kılmıştır (Küçük ve Şimşek, 2020: 613).

Dijitalleşme yoluyla sağlanan verimlilik artışı sadece işlem süreçleriyle sınırlı kalmayıp, kamu kurumlarının iç yönetim performansına da olumlu yansımaktadır. Bilgi sistemleri sayesinde kurumsal kaynak planlama, personel yönetimi ve finansal kontrol mekanizmaları daha etkin hale gelmekte, karar alma süreçleri için gerekli veriler daha kolay elde edilebilmektedir (Kaya ve Aydın, 2021:45). Bu sayede yöneticiler, kaynak dağılımını stratejik olarak optimize edebilmekte ve hizmet kalitesini yükseltebilmektedir. Ayrıca, dijitalleşme ile birlikte ortaya çıkan veri analitiği ve büyük veri uygulamaları, kamu politikalarının etkinliğini değerlendirmek ve ihtiyaçlara hızlı yanıt vermek açısından önemli araçlar olarak kullanılmaktadır (T.C. Dijital Dönüşüm Ofisi, 2023: 18).

Şeffaflık, kamu yönetiminde vatandaşların devlete olan güveninin temelini oluşturur. Dijitalleşme, kamu kurumlarının faaliyetlerinin görünür ve denetlenebilir hale gelmesini sağlayarak şeffaflık ilkesiyle doğrudan ilişkilidir. Elektronik ortamda tutulan kayıtlar, işlem geçmişi ve kurum faaliyetlerinin dijital olarak belgelenmesi, vatandaşların kamu hizmetlerine ilişkin bilgilere kolay erişimini mümkün kılmaktadır. Böylece, bilgi asimetrisi azalmakta ve vatandaşların kamu idaresine ilişkin farkındalığı artmaktadır (Heeks, 2006: 14). Türkiye'de şeffaflık ve hesap verebilirlik uygulamalarının güçlendirilmesi için geliştirilen e-Devlet sistemleri, vatandaşların dilekçe takibi, kamu

ihale süreçleri ve bütçe harcamalarına ilişkin bilgileri görüntülemesine olanak tanımaktadır (Yıldırım ve Kaya, 2023:78).

Dijital şeffaflık aynı zamanda yolsuzlukla mücadelede önemli bir araçtır. Geleneksel sistemlerde yolsuzluğa zemin hazırlayan kapalı ve takip edilemeyen süreçler, dijitalleşmeyle birlikte kayıt altına alınmakta ve denetim mekanizmaları güçlendirilmektedir. E-Devlet uygulamaları sayesinde kamu kaynaklarının kullanımına dair bilgiler şeffaflaşmakta, vatandaşlar ve denetleyici kurumlar süreçleri izleyebilmektedir (Kaya, 2022: 854). Bu durum, kamu yönetiminde güvenin artırılmasına ve kamu kaynaklarının etkin kullanımına katkı sağlamaktadır.

Hesap verebilirlik, kamu görevlilerinin ve kurumlarının yaptıkları işlemlerden dolayı kamuoyuna karşı sorumlu tutulmasıdır. Dijitalleşme, hesap verebilirlik mekanizmalarının güçlenmesinde kritik bir rol oynamaktadır. Elektronik sistemler, işlem süreçlerini otomatik olarak kaydetmekte ve raporlamalarla yöneticilerin performanslarının şeffaf biçimde izlenmesine olanak tanımaktadır (Özdemir, 2022:47). Türkiye'de e-Devlet projelerinde uygulanan dijital arşivleme ve raporlama sistemleri, denetim süreçlerinin etkinleşmesini sağlamış ve kamu yöneticilerinin sorumluluklarının netleşmesine katkı sunmuştur (Küçük ve Şimşek, 2020: 613).

Özellikle vatandaşların kamu hizmetlerine ilişkin taleplerini, şikayetlerini ve geri bildirimlerini dijital platformlar üzerinden iletebilmesi, hesap verebilirliği artıran önemli bir gelişmedir. Bu tür interaktif mekanizmalar, kamu kurumlarının hizmet kalitesini sürekli olarak iyileştirmesine olanak tanımakta ve vatandaşların kamu yönetimine aktif katılımını desteklemektedir (Yıldırım, 2022:102). Ayrıca, sosyal medya ve diğer dijital iletişim kanalları aracılığıyla kamu yöneticilerinin toplumla doğrudan etkileşim kurması, hesap verebilirliği yeni boyutlara taşımaktadır.

Dijitalleşmenin kamu yönetiminde verimlilik, şeffaflık ve hesap verebilirlik alanlarında sağladığı katkılar, kamu politikalarının kalitesini artırmakta ve demokratik yönetişimi güçlendirmektedir. Bununla birlikte, dijitalleşme sürecinde ortaya çıkan zorluklar da göz ardı edilmemelidir. Dijital altyapı eksiklikleri, dijital okuryazarlık seviyesindeki farklılıklar ve siber güvenlik riskleri, kamu yönetiminin dijitalleşme hedeflerini sınırlayan faktörlerdir (Kaya, 2022:59). Bu nedenle, dijital dönüşüm

stratejilerinde teknoloji yatırımlarının yanı sıra insan kaynağı geliştirme ve güvenlik politikalarının bütüncül bir yaklaşımla ele alınması gerekmektedir.

Türkiye özelinde değerlendirildiğinde, e-Devlet uygulamalarının yaygınlaşmasıyla birlikte kamu hizmetlerinde verimlilik önemli ölçüde artmıştır. Resmi veriler, e-Devlet Kapısı üzerinden gerçekleştirilen işlemlerin sayısının her yıl katlanarak yükseldiğini göstermekte, bu da dijitalleşmenin kamu hizmetlerine erişimde zaman ve maliyet avantajı sağladığını ortaya koymaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019:22). Şeffaflık ve hesap verebilirlik alanında da kamuoyuna sunulan dijital raporlama araçları ve geri bildirim sistemleri ile ilerleme kaydedilmiştir (Küçük ve Şimşek, 2020:613).

Dijitalleşme kamu yönetiminin temel işlevlerinin yerine getirilmesinde kritik bir dönüştürücü güç olarak ortaya çıkmaktadır. Verimlilik artışı, süreçlerin sadeleşmesi ve hızlanması; şeffaflık sayesinde kamu yönetimine olan güvenin güçlenmesi; hesap verebilirlik yoluyla yöneticilerin sorumluluklarının netleşmesi, dijitalleşmenin kamu yönetiminde yarattığı üç temel kazanımı ifade etmektedir. Bu kazanımların sürdürülebilirliği ve geliştirilmesi için teknoloji, insan kaynağı ve hukuk alanlarında eşgüdümlü çalışmaların yapılması zorunludur. Böylece Türkiye, bilgi toplumuna dönüşümünde dijital kamu yönetimi uygulamalarında örnek bir ülke konumuna yükselebilecektir.

Dijitalleşmenin kamu yönetimine sağladığı verimlilik artışının önemli bir boyutu da süreçlerin otomatikleştirilmesi ve iş yükünün azaltılmasıdır. Geleneksel bürokratik sistemlerde pek çok işlem manuel olarak yürütülmekte, bu da hem insan kaynaklarının verimsiz kullanılmasına hem de işlem sürelerinin uzamasına neden olmaktadır. Dijital teknolojiler, iş süreçlerinin otomatikleştirilmesine olanak tanıyarak çalışanların rutin işlerden kurtulmasını ve daha stratejik görevlere odaklanmasını sağlamaktadır (Heeks, 2006: 162). Örneğin, Türkiye'de uygulanan e-Devlet Kapısı'nda vatandaşların çeşitli kamu hizmetlerine ilişkin talepleri otomatik olarak yönlendirilmekte, iş süreçleri dijital iş akışlarıyla hızlandırılmaktadır (Küçük ve Şimşek, 2020: 613). Bu durum, kamu kurumlarının hizmet kapasitesini artırmakta ve kaynak kullanımında tasarruf sağlamaktadır.

Buna ek olarak, dijitalleşme kamu yönetiminde karar alma süreçlerini de köklü biçimde dönüştürmüştür. Modern bilgi sistemleri sayesinde kamu yöneticileri, büyük veri analitiği ve yapay zeka uygulamaları yoluyla daha doğru ve hızlı kararlar alabilmektedir (Tutar ve Kaya, 2023:78). Örneğin, sağlık, eğitim ve ulaşım gibi kritik alanlarda veri temelli karar destek sistemleri kullanılarak hizmetlerin etkinliği artırılmakta ve kaynakların optimum dağılımı sağlanmaktadır. Türkiye'de dijital dönüşüm stratejilerinde yapay zeka uygulamalarının yaygınlaştırılması, kamu yönetiminin performansını yükseltmek için stratejik bir hedef olarak belirlenmiştir (T.C. Dijital Dönüşüm Ofisi, 2023: 21). Bu gelişmeler, kamu kurumlarının değişen koşullara daha esnek yanıt vermesine ve vatandaş odaklı hizmet üretmesine imkân sağlamaktadır.

Dijitalleşme ile birlikte ortaya çıkan şeffaflık unsuru, kamu yönetiminde demokratik katılımın güçlenmesine de katkı sunmaktadır. Bilgiye erişim kolaylaştıkça, vatandaşlar kamu politikalarının şekillendirilmesine daha aktif biçimde katılabilmekte, görüşlerini iletebilmekte ve karar süreçlerini takip edebilmektedir (Heeks, 2006:14). Özellikle katılımcı bütçeleme ve elektronik danışma platformları gibi dijital araçlar, halkın yönetime katılımını destekleyen yenilikçi uygulamalar olarak öne çıkmaktadır (Kaya ve Aydın, 2021: 63). Türkiye'de belediyelerin dijital platformlar aracılığıyla düzenledikleri halk toplantıları ve anketler, yerel yönetimlerde şeffaflık ve hesap verebilirlik ilkelerinin hayata geçirilmesinde önemli adımlar olarak değerlendirilmektedir (Yıldırım ve Kaya, 2023: 102).

Şeffaflık ile doğrudan bağlantılı olan hesap verebilirlik ise dijitalleşme sayesinde daha sistematik ve izlenebilir hale gelmiştir. Kamu görevlilerinin sorumluluklarının net olarak belirlenmesi ve denetlenmesi, dijital kayıt sistemleri sayesinde mümkün olmaktadır (Özdemir, 2022: 47). Elektronik ortamda tutulan işlem kayıtları ve performans raporları, kamu yönetiminde yolsuzluk riskini azaltmakta ve kamu kaynaklarının doğru kullanılması konusunda denetleyici mekanizmaları güçlendirmektedir. Özellikle kamu ihale süreçlerinde kullanılan dijital platformlar, sürecin tüm aşamalarını kayıt altına almakta ve bu sayede hem şeffaflığı hem de hesap verebilirliği artırmaktadır (Kaya, 2022: 854).

Ancak dijitalleşmenin hesap verebilirlik üzerindeki etkisi sadece kurum içi denetimlerle sınırlı değildir. Vatandaşların kamu hizmetlerine ilişkin geri bildirimlerini

elektronik ortamda sunabilmesi, kamu yönetiminin performansını dışardan izleme ve değerlendirme imkânı yaratmaktadır (Yıldırım, 2022:47). Bu da kamu görevlilerinin hesap verme mekanizmasını güçlendirmekte ve kamu hizmetlerinde kaliteyi artırmaktadır. Dijital iletişim araçlarının yaygınlaşmasıyla birlikte, sosyal medya üzerinden yapılan şikayet ve öneriler, kamu kurumlarının hizmetlerini iyileştirmesinde önemli veri kaynakları haline gelmiştir.

Dijitalleşmenin kamu yönetimindeki bu olumlu etkilerine rağmen, süreç bazı zorlukları da beraberinde getirmektedir. Özellikle dijital uçurum olarak adlandırılan teknolojiye erişimdeki eşitsizlikler, bazı vatandaşların dijital hizmetlerden yeterince yararlanamamasına yol açmaktadır (Kaya, 2022:59). Bu durum, kamu hizmetlerinde kapsayıcılığın sağlanması açısından önemli bir sorun teşkil etmektedir. Ayrıca, siber güvenlik tehditleri ve veri gizliliği endişeleri, dijitalleşmenin yaygınlaştırılmasında dikkat edilmesi gereken kritik alanlardır (Özdemir ve Çelik, 2023:110). Kamu kurumlarının, bilgi güvenliği politikalarını güçlendirmesi ve vatandaşların kişisel verilerini koruma konusundaki bilinçlendirme çalışmalarını artırması gerekmektedir.

Türkiye'de dijitalleşmenin kamu yönetiminde başarıyla uygulanması için mevzuat düzenlemeleri de önemli rol oynamaktadır. KVKK gibi yasal düzenlemeler, dijital kamu hizmetlerinin güvenli ve etik bir şekilde sunulmasını temin etmektedir. Ayrıca, Dijital Dönüşüm Stratejisi kapsamında belirlenen hedefler, dijitalleşmenin kamu kurumlarında sistematik ve koordineli biçimde ilerlemesini sağlamaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019: 45).

Sonuç olarak, dijitalleşme kamu yönetiminin temel işlevlerini yeniden şekillendirirken, verimlilik, şeffaflık ve hesap verebilirlik alanlarında kayda değer gelişmeler sağlamaktadır. Ancak bu dönüşümün sürdürülebilir ve kapsayıcı olabilmesi için teknolojik altyapı yatırımları, insan kaynağı geliştirme, mevzuat uyumu ve vatandaş odaklı politikaların entegre edilmesi zorunludur. Bu yaklaşımlar, dijital kamu yönetiminin hem hizmet kalitesini yükseltmesine hem de demokratik yönetişimi güçlendirmesine olanak tanıyacaktır. Türkiye'nin dijitalleşme sürecinde bu unsurları dikkate alarak ilerlemesi, küresel bilgi toplumu içinde rekabet gücünü artıracak ve vatandaşlarının yaşam kalitesini iyileştirecektir.

İKİNCİ BÖLÜM

BİLİŞİM SUÇLARI VE KAMU YÖNETİMİ

2.1. Bilişim Kavramının ve Bilişim Suçlarının Tanımı

Bilişim kavramı, bilgisayar ve iletişim teknolojilerinin gelişimiyle ortaya çıkan ve hayatın birçok alanında etkisini gösteren çok boyutlu bir terimdir. Bilgi teknolojileri ve bilişim sistemlerinin bütününü ifade eden bilişim, verilerin toplanması, işlenmesi, depolanması, iletilmesi ve yönetilmesini sağlayan süreçleri kapsamaktadır (Kaya, 2018: 23). Bu bağlamda bilişim, sadece teknik donanım ve yazılım bileşenlerini değil, aynı zamanda bu bileşenlerin etkin bir şekilde kullanılması için gerekli olan bilgi, beceri ve süreçleri de içerir (Öztürk, 2019: 45).

Bilişim, kamu yönetimi açısından değerlendirildiğinde, devlet hizmetlerinin elektronik ortamda sunulmasını, veri tabanlarının oluşturulmasını ve yönetilmesini, ayrıca vatandaşlar ile devlet arasında dijital iletişim kanallarının kurulmasını ifade etmektedir (Demir, 2020: 67). Bu yönüyle bilişim, kamu yönetiminin etkinlik, verimlilik ve şeffaflık gibi temel değerlerine katkı sağlamaktadır (Yılmaz, 2017: 112).

Bilişim suçları ise, bilişim teknolojilerinin ve bilişim sistemlerinin kötüye kullanılmasıyla ortaya çıkan ve hukuk düzeni tarafından suç olarak tanımlanan eylemler bütünüdür. Uluslararası telekomünikasyon birliği (International Telecommunication Union - ITU) bilişim suçlarını, bilgisayar sistemleri ve ağlarına yönelik yasa dışı erişim, veri hırsızlığı, sistemlerin zarar görmesi gibi eylemler olarak tanımlamaktadır (ITU, 2015: 12). Türkiye'de ise bilişim suçlarının tanımı, 5237 sayılı TCK 'nun ilgili maddeleri ile 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da ayrıntılı şekilde ele alınmaktadır.

Bilişim suçları, klasik suç tiplerinden farklı olarak dijital ortamda işlenmekte ve teknik bilgi gerektirmektedir (Ersoy, 2016: 89). Bu suçlar, genellikle bilgi sistemlerine yetkisiz erişim, verilerin değiştirilmesi veya yok edilmesi, elektronik dolandırıcılık, kimlik hırsızlığı gibi çeşitlilik göstermektedir (Karataş, 2018: 56). Bu nedenle bilişim

suçlarının tanımlanması ve sınıflandırılması, teknolojik gelişmelerle birlikte sürekli güncellenmekte ve uluslararası normlarla uyumlu hale getirilmektedir (Smith ve Duggan, 2013:21).

Sonuç olarak, bilişim kavramı, modern kamu yönetiminin temel bileşenlerinden biri olurken; bilişim suçları, bu teknolojik altyapıya yönelik tehditler olarak ortaya çıkmaktadır. Kamu yönetiminin dijitalleşme sürecinde bilişim suçlarıyla mücadele, hem teknolojik hem de hukuki altyapının güçlendirilmesini zorunlu kılmaktadır (Yıldırım, 2021: 134).

2.2. Bilişim Suçlarının Tarihsel Gelişimi

Bilişim suçlarının ortaya çıkışı, bilgisayar teknolojilerinin gelişimi ve yaygınlaşması ile paralel bir süreç izlemektedir. İlk bilgisayarlar ve ağlar kullanılmaya başlandığında, bu teknolojik altyapı yeni suç türlerinin doğmasına zemin hazırlamıştır (Wall, 2007: 12). 1970'li yıllarda bilgisayar sistemleri sınırlı bir kullanıcı kitlesine sahip olmasına rağmen, ilk siber saldırılar bu dönemde kaydedilmiştir. Bu saldırılar genellikle sistemlere yetkisiz erişim, veri manipülasyonu ve sabotaj biçimindeydi (Holt, 2010: 22).

1980'li yıllarda internetin gelişimi ve yaygınlaşması, bilişim suçlarının tür ve boyutlarını önemli ölçüde genişletmiştir. Bu dönemde siber suçlar daha organize ve profesyonel hale gelmiş, bireysel merak veya hobi amaçlı eylemler yerini ekonomik çıkar veya siyasi motivasyonlu saldırılara bırakmıştır (Levi, 2013: 45). Özellikle devlet kurumlarına yönelik saldırılar artmış ve kritik altyapıların hedef alınmasıyla güvenlik endişeleri yükselmiştir (Holt ve Bossler, 2016: 22–23).

1990'lı yıllar, bilişim suçlarının küresel boyuta ulaştığı ve uluslararası işbirliğinin önem kazandığı bir dönem olarak kaydedilmiştir. İnternetin herkes tarafından erişilebilir hâle gelmesi, suçluların farklı coğrafyalardan hedeflere saldırabilmesine imkân tanımış ve sınır ötesi bilişim suçlarını artırmıştır (Grabosky, 2007: 10). Bu gelişmeler, ülkelerin kendi yasalarını bilişim suçlarına uyarlamasını ve uluslararası standartlarla uyum sağlamasını zorunlu kılmıştır (Broadhurst, 2006: 67).

2000'li yıllarda teknolojik gelişmeler ve mobil cihazların yaygınlaşması, bilişim suçlarının yeni boyutlarını ortaya çıkarmıştır (Yüksel, 2018: 80). Sosyal medya

platformları, bulut bilişim ve Nesnelerin İnterneti (IoT) cihazları, siber suçlular için yeni saldırı yüzeyleri oluşturmuştur (Müller, 2015: 15). Aynı zamanda fidye yazılımları (ransomware), gelişmiş kimlik avı teknikleri ve devlet destekli siber saldırılar gündeme gelmiştir (Holt ve Bossler, 2016: 25).

Türkiye özelinde bilişim suçları 2000'li yılların başından itibaren artış göstermiş ve buna bağlı olarak hukuki düzenlemeler yapılmıştır (Yıldırım, 2021: 145). 2007 yılında yürürlüğe giren 5651 sayılı İnternet Kanunu, internet ortamında işlenen suçların takibi ve cezalandırılması açısından önemli bir adım olmuştur. Ayrıca, Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Dairesi Başkanlığı'nın kurulması, bilişim suçlarına karşı mücadelede kurumsal kapasitenin artırılmasını sağlamıştır (Demir, 2020: 33).

Sonuç olarak, bilişim suçlarının tarihsel gelişimi, teknolojik ilerlemelerle şekillenmiş ve giderek karmaşıklaşmıştır. Bu süreç, uluslararası işbirliği ve ulusal mevzuatların uyumunu zorunlu kılmış, kamu yönetimi ve özel sektörün siber güvenlik alanında stratejiler geliştirmesini teşvik etmiştir (Broadhurst, 2006: 70).

2.3.Bilişim Suçu İşleme Şekilleri

Bilişim suçları, teknolojik gelişmeler ve dijitalleşmenin artmasıyla birlikte çok çeşitli yöntem ve teknikler kullanılarak işlenmektedir. Bu suçların işlenme şekilleri, bilgi sistemlerine yetkisiz erişim sağlama, verilerin değiştirilmesi veya yok edilmesi, gizlilik ihlalleri, dolandırıcılık ve kimlik hırsızlığı gibi pek çok farklı formda ortaya çıkabilmektedir (Ersoy, 2016: 89). Bilişim suçlarının çeşitliliği ve karmaşıklığı, suçluların kullandığı yöntemlerin sürekli evrilmesiyle birlikte artmaktadır (Karataş, 2018: 56).

Bilişim suçlarını işleme şekillerini sınıflandırmak, suçlarla mücadelede doğru önlemlerin alınabilmesi açısından önemlidir. Bu nedenle suç tipleri hem teknik hem de hukuki açıdan detaylı şekilde incelenmektedir (Smith ve Duggan, 2013:74). Aşağıda bilişim suçlarının en yaygın işlenme biçimleri ve teknikleri akademik literatür ışığında açıklanmaktadır.

Bu yöntemler, dijital ortamda gerçekleştirilen saldırıların kapsamını, hedeflerini ve sonuçlarını anlamaya yardımcı olurken, kamu yönetimi ve özel sektörde uygulanacak güvenlik politikalarının şekillenmesine de katkı sağlamaktadır (Yıldırım, 2021:134).

2.3.1. Çöpe Dalma (Scavenging)

Çöpe dalma, bilişim suçları kapsamında bilgi hırsızlığı yöntemlerinden biri olarak tanımlanmaktadır. İngilizce "scavenging" terimi, genel anlamıyla atık ya da kullanılmayan materyallerin toplanması anlamına gelirken, bilişim suçlarında ise kullanıcıların ya da kurumların atık olarak attığı dokümanlar, depolama birimleri veya elektronik cihazlar üzerinde bulunan bilgi kırıntılarının izinsiz olarak toplanması işlemidir (Kaya, 2018: 135).

Bu yöntem, fiziksel ortamdaki bilgilerin siber ortama taşınması veya dijital ortamda bırakılan izlerin değerlendirilmesi yoluyla gerçekleştirilebilir. Örneğin, bilgisayar kullanıcılarının yazıcı çıktılarını, silinmiş dosyaları veya kullanılmayan sabit diskleri çöpe atmaları, bu materyallerin suçlular tarafından ele geçirilip içerisindeki hassas bilgilerin kopyalanması riskini beraberinde getirir (Öztürk, 2019: 98).

Çöpe dalma suçunun temel amacı, doğrudan teknik bilgisayar sistemlerine saldırmak yerine, insan faktöründen ve fiziksel zafiyetlerden faydalanarak bilgi edinmektir. Bu yöntem, özellikle sosyal mühendislik saldırılarıyla desteklendiğinde, kurumların güvenlik açıklarını ortaya çıkarır ve geniş çaplı veri sızıntılarına yol açabilir (Yılmaz, 2017: 153).

Güvenlik açısından çöpe dalma saldırılarına karşı alınabilecek önlemler arasında, gizli ve hassas belgelerin imha edilmeden önce fiziksel olarak parçalanması, elektronik atıkların güvenli şekilde bertaraf edilmesi ve çalışanların bu konuda bilinçlendirilmesi bulunmaktadır (Demir, 2020: 78). Ayrıca, kurumların veri koruma politikalarını titizlikle uygulaması ve denetlemesi önem taşımaktadır (Ersoy, 2016: 121).

Sonuç olarak, çöpe dalma saldırıları dijital çağda hala geçerliliğini koruyan ve kurumların dikkatle ele alması gereken bir bilgi güvenliği tehdididir. Bilişim suçları bağlamında fiziksel ve dijital güvenlik önlemlerinin birlikte yürütülmesi, bu tür tehditlerin etkisini azaltmada kritik rol oynamaktadır (Yıldırım, 2021: 94).

2.3.2. Gizlice Dinleme (Sniffing)

Gizlice dinleme, ya da İngilizce karşılığıyla "sniffing", bilişim suçları kapsamında ağ trafiğini izinsiz olarak takip etmek ve veri paketlerini yakalamak anlamına gelir. Bu yöntem, genellikle bilgisayar ağlarında iletilen verilerin gizliliğini ihlal etmek amacıyla kullanılmaktadır (Holt ve Bossler, 2016: 112). Sniffing, saldırganın ağ üzerindeki veri iletişimlerini pasif veya aktif olarak dinlemesiyle gerçekleşir ve kimlik bilgileri, parola, kredi kartı bilgileri gibi hassas veriler ele geçirilebilir (Karataş, 2018: 68).

Pasif sniffing, ağdaki verileri sadece izlemek amacıyla yapılırken, aktif sniffing saldırganın ağ trafiğini manipüle ederek veri akışını değiştirmesine de olanak tanır (Smith ve Duggan, 2013:74). Özellikle kablosuz ağlarda, şifreleme kullanılmaması durumunda sniffing saldırıları daha kolay gerçekleşir ve geniş çaplı veri hırsızlıklarına sebep olabilir (Öztürk, 2019: 110).

Sniffing saldırılarına karşı alınabilecek önlemler arasında veri şifreleme, güvenli ağ protokollerinin kullanımı ve ağ üzerinde izinsiz dinleme tespit sistemlerinin kurulması yer almaktadır (Demir, 2020: 85). Ayrıca, ağ yöneticilerinin düzenli olarak ağ trafiğini izlemesi ve anormal aktiviteleri tespit etmesi kritik öneme sahiptir (Ersoy, 2016: 93).

Sonuç olarak, gizlice dinleme, bilişim suçları arasında yaygın ve etkili bir yöntem olup, özellikle kamu yönetimi ve kritik altyapılar için ciddi bir tehdit oluşturmaktadır. Bu nedenle, güvenlik önlemlerinin güçlendirilmesi ve farkındalık artırıcı eğitimlerin yapılması gerekmektedir (Yıldırım, 2021: 152).

2.3.3. Veri Aldatmacası (Data Diddling)

Veri aldatmacası, bilişim suçları kapsamında oldukça tehlikeli ve sinsi bir yöntem olarak kabul edilir. Bu suç türü, veri giriş aşamasında veya veri işlenirken bilgilerin kasıtlı olarak değiştirilmesi ya da manipüle edilmesi şeklinde tanımlanır (Ersoy, 2016: 94). Veri aldatmacası, hem bireysel hem de kurumsal sistemlerde bilgi bütünlüğünün bozulmasına yol açar ve yanlış kararların alınmasına sebep olur.

Suçlular, genellikle yetkisiz erişim sağlayarak veritabanlarında veya dosyalarda bulunan bilgileri değiştirir; örneğin bir muhasebe sisteminde finansal kayıtları manipüle edebilir ya da bir sağlık kurumunda hasta bilgilerini değiştirebilirler (Kaya, 2018: 142).

Böylece hem doğrudan maddi zararlar ortaya çıkar hem de kurumların itibarları ciddi şekilde zedelenir.

Veri aldatmacasının önlenmesi için güçlü erişim kontrolleri, veri bütünlüğü denetimleri ve sistemdeki değişikliklerin takip edilmesi (audit trail) önem taşır (Demir, 2020: 92). Ayrıca, çalışanların etik eğitimlerle bilinçlendirilmesi ve siber güvenlik politikalarının sıkı şekilde uygulanması gereklidir (Yıldırım, 2021: 156).

Kamu yönetimi açısından veri aldatmacası, karar alma süreçlerinde yanlış veri kullanılması nedeniyle hizmet kalitesini düşürmekte ve vatandaşın devlete olan güvenini sarsmaktadır. Bu nedenle özellikle kritik kamu sistemlerinde veri bütünlüğünün sağlanması hayati öneme sahiptir (Öztürk, 2019: 115).

2.3.4. Truva Atı (Trojan Horse)

Truva Atı, adını antik mitolojide yer alan meşhur hileli savaş taktiğinden alan ve bilişim suçları dünyasında yaygın olarak kullanılan bir zararlı yazılım türüdür. Bu tür yazılımlar, kullanıcıların dikkatini çekmeyen ve zararsız gibi görünen programların içerisine gizlenmiş kötü niyetli kodlar barındırır (Smith ve Duggan, 2013: 98). Kullanıcı bu programı çalıştırdığında Truva Atı etkinleşir ve bilgisayar sistemine zarar verir veya bilgileri ele geçirir.

Truva Atları genellikle e-posta ekleri, sahte yazılımlar ya da sahte güncellemeler yoluyla bulaşır. Bir kere sisteme sızdığında, arka planda gizlice çalışarak kullanıcı bilgilerini çalabilir, sistem dosyalarını bozabilir veya hackerlara erişim kapısı açabilir (Karataş, 2018: 74).

Kamu yönetiminde Truva Atları, devlet kurumlarının bilgi sistemlerine yönelik büyük tehdit oluşturur. Bu tür saldırılar, kamu hizmetlerinin aksamasına, veri kaybına ve gizli bilgilerin açığa çıkmasına neden olabilir (Ersoy, 2016: 105).

Truva Atlarına karşı savunma yöntemleri arasında güncel antivirüs yazılımlarının kullanımı, bilinmeyen kaynaklardan gelen dosyaların açılmaması, düzenli sistem taramaları ve kullanıcıların bilinçlendirilmesi yer almaktadır (Demir, 2020: 88). Ayrıca, kamu kurumlarının bilgi güvenliği politikalarını sıkı şekilde uygulaması kritik önem taşır (Yıldırım, 2021: 165).

Sonuç olarak, Truva Atları bilişim suçları içinde en tehlikeli ve sinsi yöntemlerden biri olup, kamu yönetiminde bilgi güvenliği stratejilerinin ayrılmaz parçası olmalıdır.

2.3.5. Tarama (Scanning)

Tarama, bilişim suçları alanında saldırganların hedef sistemlerdeki zayıf noktaları belirlemek amacıyla kullandıkları temel tekniklerden biridir. Bu yöntemle saldırganlar, ağ veya sistemdeki açık portları, hizmetleri ve yapılandırma hatalarını tespit ederek sızma için en uygun noktaları belirlerler (Stallings, 2017: 230). Tarama, aktif veya pasif olabilir; aktif taramada doğrudan hedefe yönelik paketler gönderilerek sistem tepkileri analiz edilirken, pasif taramada ağ trafiği gizlice gözlemlenir (Whitman ve Mattord, 2018: 75).

Tarama teknikleri arasında port tarama (port scanning), ağ tarama (network scanning), güvenlik açıkları tarama (vulnerability scanning) yer almaktadır. Bu yöntemler sayesinde saldırganlar sistemde çalışan servislerin sürümleri, açıklar ve potansiyel zafiyetleri öğrenerek daha hedefli saldırılar gerçekleştirirler (Kim ve Solomon, 2016: 142).

Kamu yönetiminde, kritik altyapılarda ve bilgi sistemlerinde yapılan taramalar, kötü niyetli kişiler tarafından kullanıldığında, bilgi sızıntısına ve sistemlerin ele geçirilmesine neden olabilir. Özellikle devlet kurumlarının altyapılarında güvenlik zafiyetlerinin belirlenmesi ve kapatılması hayati önem taşır (Demir, 2020: 95).

Tarama saldırılarına karşı alınacak önlemler arasında firewall ve IDS/IPS sistemlerinin etkin kullanımı, düzenli güvenlik taramalarının yapılması, sistemlerin güncel tutulması ve ağ trafiğinin izlenmesi bulunmaktadır (Ersoy, 2016: 118). Ayrıca, kamu çalışanlarının siber güvenlik konusunda bilinçlendirilmesi ve güvenlik politikalarının uygulanması gereklidir (Yıldırım, 2021:172).

Sonuç olarak, tarama yöntemleri bilişim suçlarında ön hazırlık aşaması olarak kritik bir rol oynamakta olup, kamu yönetiminde sistem güvenliğinin sağlanması için taramalara karşı aktif savunma mekanizmalarının kurulması zorunludur.

2.3.6. Süper Darbe (Super Zapping)

Süper Darbe, bilişim suçları kapsamında oldukça karmaşık ve yıkıcı bir saldırı türüdür. Bu saldırı, genellikle yüksek yetkili kullanıcılar tarafından, sistemde bulunan kritik verilerin silinmesi veya değiştirilmesi amacıyla gerçekleştirilir (Ersoy, 2016: 121).

Süper Darbe terimi, sistem üzerinde kontrol sahibi olan bir kullanıcının kötü niyetle yaptığı müdahaleleri ifade eder; örneğin, bir sistem yöneticisinin yetkilerini kötüye kullanarak önemli verileri yok etmesi veya değiştirmesi bu kapsama girer (Demir, 2020: 100).

Süper Darbe saldırıları, özellikle kamu kurumlarında bilgi güvenliğinin ihlal edilmesine, veri kaybına ve kamu hizmetlerinin aksamasına yol açabilir. Süper Darbe saldırılarının önlenmesi, erişim kontrollerinin sıkı tutulması, yetki seviyelerinin dikkatli yönetilmesi ve sistem aktivitelerinin sürekli izlenmesi ile mümkündür (Kaya, 2018: 155).

Bu saldırılar genellikle iç tehdit kategorisinde değerlendirilir. İçeriden gelen saldırılar, dışarıdan yapılan saldırılara kıyasla daha zor tespit edilir ve önlenir, çünkü yetkili kullanıcıların sistemlere erişimi bulunmaktadır (Yıldırım, 2021: 189). Bu nedenle kamu kurumlarında yetki yönetimi ve kullanıcı davranışlarının analizi kritik öneme sahiptir.

Güvenlik politikaları kapsamında, yetkilendirme süreçlerinin düzenlenmesi, kullanıcı faaliyetlerinin loglanması ve düzenli denetimlerin yapılması Süper Darbe saldırılarını azaltmak için etkili yöntemlerdir (Öztürk, 2019: 125). Ayrıca, personel eğitimi ve farkındalık programları da bu tür saldırıların önlenmesinde önemli rol oynar.

Sonuç olarak, Süper Darbe saldırıları kamu yönetiminde bilgi güvenliğine yönelik ciddi bir tehdit olup, kurumların iç güvenlik politikalarını güçlendirmesi gerekmektedir.,

2.3.7. Salam Tekniği (Salami Techniques)

Salam Tekniği, bilişim suçları arasında oldukça sinsi ve küçük miktarlarda zarar veren bir saldırı biçimidir. Adını, büyük bir salamın ince dilimlere bölünerek yavaş yavaş tüketilmesine benzetilen bu yöntem, sistemlerden küçük ama sürekli miktarlarda veri veya para çalmak amacıyla kullanılır (Ersoy, 2016: 124). Bu teknik, bireysel işlemlerde fark edilmesi zor olduğu için saldırganlar tarafından tercih edilir.

Salam Tekniği genellikle finansal sistemlerde, bankacılık ve kamu yönetimindeki muhasebe uygulamalarında ortaya çıkar. Örneğin, sistemde gerçekleşen her işlemden birkaç kuruşun ya da küçük bir yüzdelik oranın gizlice saldırganın hesabına aktarılması şeklinde uygulanabilir (Kaya, 2018: 160). Bu küçük kayıplar, uzun vadede büyük maddi zararlara yol açar ve tespit edilmesi oldukça zordur.

Kamu yönetiminde bu tür saldırılar, kamu kaynaklarının yanlış kullanımı ve bütçe açıklarıyla sonuçlanabilir. Bu nedenle, sistemlerin güvenlik kontrollerinin ve denetim mekanizmalarının sıkı olması gerekmektedir (Demir, 2020: 104). Ayrıca, şeffaflık ve hesap verebilirliğin sağlanması için işlemlerin düzenli olarak denetlenmesi büyük önem taşır (Yıldırım, 2021: 192).

Salam Tekniği' ne karşı alınabilecek önlemler arasında, işlem kayıtlarının detaylı incelenmesi, anormallik tespiti için veri madenciliği tekniklerinin kullanılması ve güçlü iç kontrol mekanizmalarının oluşturulması yer alır (Öztürk, 2019: 130).

Sonuç olarak, Salam Tekniği, küçük miktarlarda yapılan sürekli hileler nedeniyle saptanması güç olan ama maddi açıdan ciddi zararlar doğuran bir bilişim suçu türüdür. Kamu yönetimi açısından etkili denetim sistemleri ile bu tür saldırıların önüne geçilmesi mümkün olmaktadır.

2.3.8. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

Hacking, bilişim suçları arasında en bilinen ve yaygın yöntemlerden biridir. Sistem güvenliğinin kırılması anlamına gelen hacking, yetkisiz kişilerin bilgisayar sistemlerine veya ağlara erişim sağlayarak veri çalma, değiştirme, yok etme veya sistemleri kontrol etme faaliyetlerini kapsar (Whitman ve Mattord, 2018: 85). Hacking saldırıları, bireysel kullanıcılar kadar kamu kurumları için de büyük tehdit oluşturur.

Hackerlar, zafiyetleri keşfederek bu açıkları kullanır ve sistemlere sızar. Bu süreçte parola kırma, sosyal mühendislik, zararlı yazılım yerleştirme gibi birçok yöntem kullanılır (Stallings, 2017: 250). Kamu yönetiminde kritik bilgilerin bulunduğu sistemlerin hacklenmesi, devlet sırlarının açığa çıkması, hizmetlerin aksaması ve vatandaşların kişisel bilgilerinin çalınması gibi ciddi sonuçlara yol açabilir (Demir, 2020: 110).

Kamu kurumlarının sistemlerinin hacklenmesini önlemek için çok katmanlı güvenlik önlemleri almak gereklidir. Bunlar arasında güçlü parola politikaları, çok faktörlü kimlik doğrulama, düzenli sistem güncellemeleri ve güvenlik duvarları bulunur (Kim ve Solomon, 2016: 160). Ayrıca, çalışanların siber güvenlik eğitimi alması ve şüpheli aktivitelerin anlık olarak izlenmesi büyük önem taşır (Yıldırım, 2021: 205).

Hacking, sadece dış tehditlerden değil, içeriden gelen kötü niyetli kullanıcılar tarafından da gerçekleştirilebilir. Bu nedenle, erişim kontrollerinin ve yetkilendirme sistemlerinin etkin şekilde uygulanması gerekir (Ersoy, 2016: 120).

Sonuç olarak, hacking kamu yönetiminde bilgi güvenliği açısından en kritik tehditlerden biridir ve buna karşı etkili savunma stratejilerinin geliştirilmesi zorunludur.

2.3.9. Gizli (Tuzak) Kapılar (Trap Doors)

Gizli kapılar veya trap doors, bilişim sistemlerinde geliştiriciler tarafından kasıtlı olarak yerleştirilen veya kötü niyetli saldırganlar tarafından sonradan eklenen gizli erişim noktalarıdır. Bu kapılar, yetkisiz kullanıcıların sistemlere müdahale etmesini sağlar ve genellikle sistemin güvenlik mekanizmalarını atlayarak doğrudan erişim imkanı sunar (Stallings, 2017: 270).

Trap door kavramı, özellikle kamu yönetimi gibi kritik bilgi sistemlerinde ciddi risk oluşturur. Eğer kötü niyetli kişiler bu gizli kapıları tespit edip kullanabilirse, sistem verilerine izinsiz erişebilir, verileri değiştirebilir veya sistemi tamamen ele geçirebilirler (Demir, 2020: 115). Bu tür arka kapılar, sistemin bütünlüğünü ve gizliliğini tehdit eder.

Gizli kapıların tespiti zordur çünkü normal kullanıcılar tarafından fark edilmez ve sistem üzerinde yetkili kişiler tarafından bile çoğu zaman bilinmez. Bu nedenle, yazılım geliştirme sürecinde ve sistem yönetiminde katı güvenlik standartlarının uygulanması zorunludur (Kim ve Solomon, 2016: 175).

Kamu kurumlarında bu tür risklerin önlenmesi için sistemlerde düzenli güvenlik taramaları yapılmalı, kod denetimleri gerçekleştirilmeli ve üçüncü taraf yazılımların kullanımı sıkı kontrol edilmelidir (Yıldırım, 2021: 220). Ayrıca, sistemlerin izinsiz erişimlere karşı sürekli olarak izlenmesi ve olağan dışı aktivitelerin raporlanması gereklidir (Ersoy, 2016: 130).

Sonuç olarak, trap doors kamu yönetiminde bilgi güvenliği açısından büyük tehlike arz eder ve önlenmesi için gelişmiş güvenlik politikaları ve teknikleri uygulanmalıdır.

2.3.10. Ağ Solucanları (Network Worms)

Ağ solucanları, bilgisayar ağlarında kendini çoğaltarak yayılan ve sistemlere zarar veren kötü amaçlı yazılımlardır (Whitman ve Mattord, 2018: 215). Solucanlar, genellikle

güvenlik açıklarını kullanarak ağdaki diğer bilgisayarlara bulaşır ve bu şekilde hızlı bir yayılım gösterir. Kamu yönetimindeki bilgi sistemlerinde solucan saldırıları, hem hizmet kesintilerine hem de veri güvenliği ihlallerine yol açabilir.

Solucanlar, bulaştıkları sistemlerin performansını düşürür, veri kaybına sebep olabilir ve bazen sistemlerin tamamen çökmesine neden olabilir (Stallings, 2017: 285). Bu tür saldırılar, kritik kamu hizmetlerinin kesintiye uğramasına yol açarak vatandaşların devletle olan etkileşimlerini olumsuz etkiler. Örneğin, sağlık, eğitim ya da güvenlik alanlarında kullanılan sistemlerin solucanlar tarafından etkilenmesi ciddi sonuçlar doğurabilir.

Kamu kurumları, ağ solucanlarına karşı etkili savunma mekanizmaları geliştirmek zorundadır. Bu mekanizmalar arasında düzenli yazılım güncellemeleri, antivirüs programları, ağ trafiğinin sürekli izlenmesi ve saldırı tespit sistemlerinin kullanılması yer alır (Kim ve Solomon, 2016: 180). Ayrıca, personelin siber güvenlik konusunda eğitilmesi ve farkındalık yaratılması da önemlidir.

Solucan saldırılarının önlenmesi, kamu yönetiminin dijitalleşme sürecinde bilgi güvenliğinin sağlanması için kritik bir faktördür. Çünkü ağ solucanlarının hızlı yayılımı, devletin dijital hizmetlerini sekteye uğratabilir ve vatandaş güvenini zedeleyebilir (Yıldırım, 2021: 225).

Sonuç olarak, ağ solucanları kamu yönetiminde ciddi tehditler arasında yer almakta ve bu tehditlere karşı kapsamlı güvenlik stratejilerinin geliştirilmesi gerekmektedir.

2.3.11. Bilgisayar Virüsleri

Bilgisayar virüsleri, zararlı yazılımlar arasında en yaygın bilinen türlerden biridir ve kamu yönetimi bilgi sistemleri için ciddi tehditler oluşturur. Virüsler, kendilerini çoğaltarak sistemlere zarar verir, dosyaları bozabilir, sistem performansını düşürebilir ve hassas bilgilerin çalınmasına yol açabilir (Ersoy, 2016: 135). Kamu kurumlarının kritik verilerinin hedef alınması, vatandaşların hizmetlere erişimini engelleyebilir ve güvenlik açıklarına neden olabilir.

Bilgisayar virüsleri farklı türlerde olabilir: dosya virüsleri, boot virüsleri, makro virüsleri gibi (Stallings, 2017: 300). Virüsler, genellikle e-posta ekleri, internetten

indirilen dosyalar ya da taşınabilir bellekler aracılığıyla yayılır. Kamu yönetiminde, virüs bulaşan sistemlerin hizmet dışı kalması hem iş sürekliliğini etkiler hem de kurumun itibarı zarar görür (Demir, 2020: 120).

Virüslere karşı korunmak için düzenli antivirüs güncellemeleri, güvenlik yazılımlarının etkin kullanımı ve personelin bilinçlendirilmesi gereklidir (Kim ve Solomon, 2016: 190). Ayrıca, kamu kurumlarında güvenli internet kullanımı ve veri yedekleme politikaları uygulanmalıdır.

Virüsler, sadece sistemleri değil, aynı zamanda kamu yönetiminin dijitalleşme süreçlerini de olumsuz etkiler. Bu nedenle, kamu kurumlarının bilgi güvenliği stratejilerini sürekli güncelleyerek virüslere karşı savunma mekanizmalarını güçlendirmesi önemlidir (Yıldırım, 2021: 230).

Sonuç olarak, bilgisayar virüsleri kamu yönetiminde bilgi güvenliği açısından kritik riskler oluşturur ve etkin önlemlerle bu tehditlerin minimize edilmesi gerekmektedir.

2.3.12. Mantık Bombaları (Logic Bombs)

Mantık bombaları, belirli bir koşulun gerçekleşmesi durumunda aktif hale gelen kötü amaçlı yazılım türleridir. Bu yazılımlar, sisteme zarar vermek, veri kaybına yol açmak veya sistemin işleyişini bozmak amacıyla programlanır (Whitman ve Mattord, 2018: 230). Kamu yönetiminde mantık bombalarının kullanılması, kritik devlet verilerinin zarar görmesi, hizmetlerin aksaması ve kamu güveninin sarsılması gibi sonuçlar doğurabilir.

Mantık bombaları genellikle bir olayın gerçekleşmesi (örneğin belirli bir tarihe gelinmesi veya bir programın çalıştırılması) üzerine devreye girer. Bu nedenle tespiti zor ve etkileri ani olur (Stallings, 2017: 310). Kamu kurumlarının sistemlerinde yer alan bu tür zararlı kodların tespiti için düzenli kod incelemeleri ve güvenlik taramaları yapılması gerekir (Demir, 2020: 125).

Mantık bombalarının kamu yönetimindeki etkileri, bilgi sistemlerinin güvenilirliğini tehdit eder ve dijitalleşme sürecinde ciddi riskler oluşturur. Bu nedenle, kamu kurumlarının bilişim sistemlerinde kapsamlı güvenlik önlemleri alması ve personel eğitimi ile farkındalık artırılması hayati önem taşır (Kim ve Solomon, 2016: 195).

Sonuç olarak, mantık bombaları kamu yönetimi bilgi sistemlerinde ciddi tehdit oluşturan bilişim suçları arasında yer almakta ve etkili tespit ve önlem yöntemlerinin geliştirilmesi gerekmektedir.

2.3.13. İstem Dışı Alınan E-Postalar (Spam)

Spam, istem dışı gönderilen e-postalar veya dijital iletişim mesajlarıdır ve kamu yönetiminde bilgi güvenliğini tehdit eden önemli sorunlardan biridir. Spam mesajlar, genellikle reklam, dolandırıcılık veya kötü amaçlı yazılım içerir ve kullanıcıların iş verimliliğini düşürmenin yanı sıra sistemlerin güvenliğini de riske atar (Stallings, 2017: 320). Kamu kurumlarında spam, bilgi sistemlerinin işleyişini engelleyebilir, önemli mesajların gözden kaçmasına neden olabilir ve ağ kaynaklarının gereksiz yere tüketilmesine yol açabilir.

Spam mesajlar aynı zamanda phishing (oltalama) saldırıları için bir araç olarak kullanılabilir. Dolandırıcılar, sahte e-postalarla kullanıcıları kişisel bilgilerini vermeye ya da zararlı yazılımları çalıştırmaya yönlendirebilirler (Kim ve Solomon, 2016: 210). Bu durum, kamu yönetiminde veri güvenliği açısından kritik riskler doğurur.

Kamu kurumları, spam ile mücadelede etkili filtreleme sistemleri kullanmalı, e-posta güvenliğini artırmalı ve personelin bilinçlendirilmesini sağlamalıdır (Yıldırım, 2021: 245). Ayrıca, düzenli güncellemeler ve güvenlik yamaları spam saldırılarını önlemede önemli rol oynar.

Sonuç olarak, spam, kamu yönetiminde bilişim suçlarına zemin hazırlayan bir faktör olup, etkili mücadele yöntemleri geliştirilerek bilgi güvenliği sağlanmalıdır.

2.3.14. Oltalama Saldırısı (Phishing Attacks)

Oltalama saldırıları (phishing), kötü niyetli kişilerin sahte e-postalar, web siteleri veya diğer iletişim araçları aracılığıyla kullanıcıların kişisel bilgilerini, şifrelerini ya da finansal verilerini ele geçirmeye yönelik saldırılardır. Kamu yönetiminde, bu tür saldırılar hem vatandaşların hem de kurum çalışanlarının hassas bilgilerini tehlikeye atarak ciddi güvenlik ihlallerine yol açabilir (Whitman ve Mattord, 2018: 245).

Phishing saldırıları genellikle güvenilir kurumlar veya kişiler taklit edilerek gerçekleştirilir ve kullanıcılar kandırılarak sahte bağlantılara yönlendirilir (Kim ve

Solomon, 2016: 215). Bu saldırılar, kamu hizmetlerine erişimi sağlayan dijital platformlarda bilgi hırsızlığına ve hizmetlerin kötüye kullanılmasına neden olabilir.

Kamu kurumlarının, phishing saldırılarına karşı çalışanlarına düzenli eğitimler vermesi, gelişmiş filtreleme sistemleri kullanması ve kullanıcıların bilinçlendirilmesi gereklidir (Yıldırım, 2021: 250). Ayrıca, güvenli doğrulama yöntemleri (iki faktörlü kimlik doğrulama gibi) bu tür saldırıların etkisini azaltabilir.

Sonuç olarak, oltalama saldırıları kamu yönetiminde dijitalleşmenin önemli tehditlerinden biridir ve bu tehdide karşı kapsamlı stratejiler geliştirilmesi zorunludur.

2.3.15. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme

Web sayfası hırsızlığı, bir web sitesinin tasarımının, içeriğinin veya işlevselliğinin izinsiz olarak kopyalanmasıdır. Bu durum, kamu yönetimi dijital platformları için önemli bir tehdit oluşturur çünkü vatandaşlara sunulan resmi hizmetlerin güvenilirliği ve kurumların itibarı zarar görebilir (Ersoy, 2016: 140). Hırsızlık yoluyla elde edilen web içerikleri, sahte web siteleri oluşturmak ve kullanıcıları yanlış yönlendirmek için kullanılabilir.

Web sayfası yönlendirme ise, kullanıcıların orijinal siteleri yerine kötü niyetli veya sahte sitelere yönlendirilmesini sağlayan bir siber saldırı yöntemidir (Stallings, 2017: 330). Kamu kurumlarının dijital hizmetlerine erişmek isteyen vatandaşlar, bu tür saldırılar sonucunda sahte sitelere düşerek kişisel bilgilerini tehlikeye atabilirler.

Bu tür saldırılara karşı kamu kurumlarının, web sitelerinin düzenli olarak güncellenmesi ve güvenlik açıklarının hızlı bir şekilde kapatılması gerekmektedir (Kim ve Solomon, 2016: 220). Ayrıca, kullanıcıların resmi web adreslerini doğrulamaları için bilinçlendirilmesi de önemlidir.

Sonuç olarak, web sayfası hırsızlığı ve yönlendirme saldırıları, kamu yönetiminde dijital güvenliğin sağlanması için önemli riskler arasında yer almakta ve bu risklerin önlenmesi için etkin önlemler alınmalıdır.

2.3.16. Hukuka Aykırı İçerik Sunma

Hukuka aykırı içerik sunma, bilişim suçları kapsamında kamu yönetimi için ciddi bir tehdit oluşturur. Bu durum, kamu kurumlarının dijital platformlarında yasalarla korunan normlara aykırı, zararlı, yanlış bilgilendirici veya etik dışı içeriklerin yayılması

anlamına gelir (Ersoy, 2016: 145). Özellikle sosyal medya ve resmi web siteleri gibi dijital kanallar, yanlış bilginin hızla yayılmasına ve toplumda güvensizlik yaratılmasına zemin hazırlayabilir.

Bu tür içerikler, kamu yönetiminin itibarını zedeleyebilir ve vatandaşlar arasında karmaşaya neden olabilir. Ayrıca, terör propagandası, nefret söylemi ve dezenformasyon gibi hukuka aykırı içerikler, toplumsal barışı ve kamu düzenini tehdit eder (Whitman ve Mattord, 2018: 255).

Kamu kurumları, hukuka aykırı içeriklerin tespiti ve engellenmesi için teknik altyapılar geliştirmeli, içerik izleme sistemleri kurmalı ve gerekli durumlarda hukuki işlemleri başlatmalıdır (Demir, 2020: 130). Ayrıca, vatandaşların doğru bilgiye erişimini sağlamak amacıyla şeffaf ve etkili iletişim stratejileri geliştirilmelidir.

Sonuç olarak, hukuka aykırı içerik sunma, kamu yönetiminde dijitalleşmenin yarattığı yeni risklerden biri olup, bu risklere karşı etkin mücadele mekanizmalarının kurulması gerekmektedir.

2.3.17. Ortadaki (Aradaki) Adam Saldırısı (Man in the Middle Attack)

Ortadaki adam saldırısı (Man in the Middle - MITM), iki taraf arasındaki iletişimi gizlice dinleyip, değiştiren veya yönlendiren bir siber saldırı türüdür. Bu saldırı, kamu yönetiminde kullanılan bilgi sistemleri için büyük bir tehdit oluşturur çünkü hassas bilgilerin ele geçirilmesi, veri bütünlüğünün bozulması ve kimlik doğrulama süreçlerinin atlatılması gibi sonuçlar doğurabilir (Whitman ve Mattord, 2018: 260).

MITM saldırıları genellikle, kamu kurumlarının internet üzerindeki iletişim kanallarını hedef alır ve kullanıcı ile sunucu arasındaki veri transferini araya girerek kontrol altına almaya çalışır (Kim ve Solomon, 2016: 225). Bu tür saldırılar, özellikle halka açık Wi-Fi ağlarında ve zayıf şifreleme kullanılan ortamlarda yaygındır.

Kamu yönetiminde MITM saldırılarını önlemek için güçlü şifreleme protokolleri (SSL/TLS), VPN kullanımı ve iki faktörlü kimlik doğrulama yöntemleri uygulanmalıdır (Stallings, 2017: 345). Ayrıca, personel eğitimi ve farkındalık artırma çalışmaları da bu tür saldırılara karşı etkili savunma mekanizmalarıdır.

Sonuç olarak, Ortadaki Adam saldırıları, kamu yönetiminde dijital güvenlik alanında önemli bir tehdit olarak varlığını sürdürmekte ve bu tehdide karşı kapsamlı teknik ve idari önlemler alınması gerekmektedir.

2.4. Kamu Yönetiminde Bilişim Suçlarının Etkileri

Günümüzde bilişim teknolojilerinin kamu yönetiminde yaygın şekilde kullanılması, kamu hizmetlerinin etkinliği ve erişilebilirliğinde önemli gelişmeler sağlamıştır. Ancak, bilişim suçları kamu yönetiminin işleyişi ve güvenliği açısından ciddi tehditler oluşturmaktadır (Kumar ve Sharma, 2020: 45). Bilişim suçları, sadece bireysel zararlar yaratmakla kalmayıp, devlet kurumlarının veri güvenliği, kamu hizmetlerinin sürekliliği ve vatandaşların devletle olan etkileşimlerini de olumsuz etkileyebilmektedir (Altun ve Demir, 2021: 62).

Kamu yönetiminde bilişim suçlarının etkilerini anlamak için öncelikle bu suçların kapsamı ve ortaya çıkış biçimleri incelenmelidir. Bilişim suçları, siber saldırılar, veri hırsızlığı, sistemlere yetkisiz erişim, kamu kurumlarının web sitelerine yönelik saldırılar, fidye yazılımları ve bilgi manipülasyonu gibi çok çeşitli şekillerde ortaya çıkabilmektedir (Sarı ve Kaya, 2019: 34). Bu tür suçların yaygınlaşması, kamu kurumlarının bilgi işlem altyapılarının güvenliğini artırma ihtiyacını doğurmuştur (Yılmaz, 2022: 15).

Bilişim suçlarının kamu yönetimine etkileri çok boyutludur. İlk olarak, kamu hizmetlerinin kesintiye uğraması önemli bir sorundur. Özellikle sağlık, eğitim, ulaşım gibi kritik alanlarda faaliyet gösteren kamu kurumlarının bilişim sistemlerine yapılan saldırılar, hizmetlerin durmasına veya aksamasına neden olmaktadır (Öztürk, 2020: 18). Bu durum, vatandaşların devlet hizmetlerine erişimini zorlaştırmakta ve kamuya olan güveni azaltmaktadır (Demirtaş ve Yıldız, 2021: 44).

İkinci olarak, kamu yönetiminde veri güvenliği konusu öne çıkmaktadır. Bilişim suçları kapsamında gerçekleştirilen veri hırsızlıkları, kişisel ve kurumsal bilgilerin açığa çıkmasına yol açmakta, bu da hem bireylerin hem de devletin zarar görmesine neden olmaktadır (Aydın, 2019: 92). Özellikle kişisel verilerin korunması açısından devletin sorumluluğu büyük olup, bu verilerin kötüye kullanılması hukuki ve sosyal sorunları beraberinde getirmektedir (Çelik, 2021: 110).

Üçüncü olarak, bilişim suçlarının kamu yönetimi üzerindeki ekonomik etkileri büyüktür. Siber saldırıların önlenmesi, zararların giderilmesi ve sistemlerin iyileştirilmesi

için kamu kaynaklarından önemli bütçeler ayrılmaktadır (Tekin, 2020: 67). Ayrıca, bilişim suçları nedeniyle ortaya çıkan hizmet aksaklıkları dolayısıyla doğrudan ve dolaylı ekonomik kayıplar yaşanmaktadır (Karaca, 2019: 52).

Bilişim suçlarının kamu yönetimindeki etkileri sadece teknik ve ekonomik boyutlarla sınırlı kalmamaktadır. Sosyal ve psikolojik etkileri de önemli bir yer tutmaktadır. Kamu kurumlarına yönelik siber saldırılar, toplumda güvenlik kaygılarının artmasına ve devlet otoritesine duyulan güvenin azalmasına yol açabilmektedir (Demir ve Ersoy, 2020: 45). Bu durum, vatandaşların devletle olan etkileşimlerini olumsuz yönde etkileyerek, kamu hizmetlerinden faydalanma oranlarını düşürebilmektedir (Yalçın, 2022: 89).

Sonuç olarak, bilişim suçları kamu yönetiminin işleyişinde çok katmanlı ve derin etkiler yaratmaktadır. Kamu kurumlarının güvenlik stratejilerini sürekli güncellemeleri, personel eğitimine önem vermeleri ve teknolojik altyapılarını güçlendirmeleri gerekmektedir (Kara ve Gündüz, 2021: 103). Ayrıca, bu alanda yasal düzenlemelerin de çağın gereksinimlerine uygun olarak geliştirilmesi önem arz etmektedir (TÜBİTAK, 2018: 27).

Bilişim suçlarının kamu yönetimi üzerindeki etkileri sadece doğrudan fiziksel veya dijital zararla sınırlı değildir; aynı zamanda kamu politikalarının oluşturulması, karar alma süreçleri ve devletin vatandaşlarla olan ilişkilerinde de önemli sonuçlar doğurmaktadır (Smith ve Jones, 2019: 112). Özellikle, kamu yönetiminin şeffaflık ve hesap verebilirlik ilkesine zarar veren bu tür suçlar, kamuoyunun devlet kurumlarına olan güveninin azalmasına sebep olmaktadır (Erdoğan ve Altay, 2020: 78).

Birçok kamu kurumu, kritik altyapıların yönetiminde dijital sistemlere dayanmakta olup, bu sistemlerin hedef alınması kamu hizmetlerinin sürekliliğini tehdit etmektedir (Brown ve Wilson, 2021: 45). Örneğin, sağlık sektöründe kullanılan elektronik hasta kayıt sistemlerine yönelik saldırılar, hasta verilerinin kaybolması veya kötüye kullanılması riskini artırmaktadır (Toprak, 2020: 33). Bu durum, sadece hastaların özel hayatlarının ihlali anlamına gelmemekte, aynı zamanda acil sağlık hizmetlerinin aksamasına da yol açabilmektedir (Özdemir, 2021: 50).

Kamu yönetiminde bilişim suçlarının bir diğer önemli etkisi de yasal ve etik sorunların ortaya çıkmasıdır. Veri ihlalleri ve siber saldırılar, devletin bireysel hakları

koruma sorumluluğunu zedelemekte, kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin etkinliğinin sorgulanmasına neden olmaktadır (Yavuz, 2019: 60). Türkiye'de KVKK gibi düzenlemeler bu alanda önemli bir rol oynasa da, uygulamada karşılaşılan zorluklar ve eksiklikler bilişim suçlarının etkilerini artırmaktadır (Kara ve Şahin, 2022: 88).

Bilişim suçları, kamu yönetiminin stratejik hedeflerine ulaşmasını da olumsuz etkiler. Siber tehditler karşısında kamu kurumlarının kaynaklarını risk yönetimine ve güvenlik önlemlerine yönlendirmesi, diğer temel hizmetlere ayrılacak kaynakların kısıtlanmasına yol açmaktadır (Lee ve Park, 2020: 102). Bu da kamu hizmetlerinin kalitesinde azalma ve inovasyon kapasitelerinde gerileme olarak kendini gösterebilir (Demirci, 2021: 75).

Siber suçların kamu yönetimine etkileri, sadece devletin iç işleyişi ile sınırlı kalmaz; aynı zamanda uluslararası ilişkilerde de önemli sonuçlar doğurabilir. Özellikle uluslararası siber casusluk ve saldırılar, devletlerin birbirine olan güvenini sarsmakta, diplomatik ilişkilerde krizlere neden olmaktadır (Morgan, 2019:45). Türkiye gibi jeopolitik açıdan kritik ülkeler için bu tehditler daha da kritik bir hal almaktadır (Özcan, 2022:72).

Kamu kurumlarının bu tehditlere karşı geliştirdiği savunma mekanizmaları da bilişim suçlarının etkisini azaltmada hayati önem taşımaktadır. Siber güvenlik politikalarının etkin uygulanması, kurumların donanım ve yazılım altyapılarının sürekli güncellenmesi, personelin farkındalık eğitimleri ve kriz yönetimi stratejileri, kamu yönetiminin dirençliliğini artırmaktadır (Smith, 2021: 88). Ancak, bu alanlarda yaşanan yetersizlikler bilişim suçlarının kamu hizmetlerine verdiği zararı büyütmektedir (Gürkan ve Yılmaz, 2020: 110).

Bilişim suçlarının kamu yönetimine etkilerinin değerlendirilmesinde, vaka analizleri önemli yer tutar. Örneğin, 2017 yılında yaşanan WannaCry fidye yazılımı saldırısı, birçok kamu kurumunun bilgisayar sistemlerini kilitlemiş ve kritik kamu hizmetlerinin aksamasına neden olmuştur (Kumar ve Singh, 2018: 102). Türkiye'de de benzer saldırılar bazı belediyeler ve kamu sağlık kuruluşlarında yaşanmış, bu olaylar kamu yönetiminde siber güvenlik önlemlerinin artırılması gerektiğini göstermiştir (Çetin, 2020: 75).

Bilişim suçlarının kamu yönetiminde yarattığı etkiler üzerine yapılan araştırmalar, bu tehditlerin artan bir hızla yaygınlaştığını ve giderek daha karmaşık hale geldiğini ortaya koymaktadır (TÜBİTAK, 2023: 45). Bu nedenle, kamu kurumlarının sadece teknik önlemler almakla kalmayıp, aynı zamanda hukuk, eğitim ve politika alanlarında da bütüncül yaklaşımlar geliştirmeleri gerekmektedir (Yılmaz ve Demir, 2022: 88).

Ek olarak, kamu yönetiminde bilişim suçlarının etkilerinin ölçülmesi ve raporlanması da önem taşımaktadır. Sistematik analizler ve performans göstergeleri oluşturulması, kamu kurumlarının riskleri daha iyi yönetmesini ve önleyici stratejiler geliştirmesini mümkün kılmaktadır (Öztürk ve Kaya, 2021: 112). Böylece, hem güvenlik açıkları minimize edilmekte hem de kamu hizmetlerinin kesintisiz devamlılığı sağlanmaktadır (Acar, 2020: 59).

Özetle, bilişim suçlarının kamu yönetimine etkileri çok yönlü ve derindir. Bu suçların oluşturduğu riskler sadece teknolojik değil, ekonomik, hukuki ve sosyal boyutlarda da hissedilmektedir. Kamu yönetimi, bu tehditlerle mücadelede teknoloji kullanımını etkinleştirmekle kalmayıp, aynı zamanda insan faktörünü de ön planda tutan kapsamlı politikalar geliştirmelidir (Yıldırım, 2021: 74). Türkiye'nin bu alandaki mevzuat ve altyapı yatırımlarını artırması, ulusal güvenlik ve kamu hizmetlerinin sürdürülebilirliği açısından kritik önem taşımaktadır (TÜBİTAK, 2023: 33).

Bilişim suçlarının kamu yönetiminde oluşturduğu en kritik sorunlardan biri, devletin vatandaşlara sunduğu hizmetlerin sürekliliğinin tehdit edilmesidir. Dijitalleşmenin artmasıyla birlikte kamu hizmetlerinin büyük bir kısmı elektronik ortamda sunulmakta, bu da hizmetlerin güvenliğinin sağlanmasını zorunlu kılmaktadır (Özkan ve Yıldız, 2020: 88). Siber saldırılar nedeniyle yaşanan hizmet aksaklıkları, vatandaşların kamu kurumlarına olan güvenini azaltmakta ve devletin meşruiyetine zarar verebilmektedir (Turan ve Kara, 2019: 102). Özellikle seçim dönemleri ve kritik kamu politikalarının uygulandığı süreçlerde bilişim suçları nedeniyle yaşanan kesintiler, demokratik işleyişi zayıflatmakta ve kamu düzenini olumsuz etkilemektedir (Çoban ve Demirtaş, 2021: 76).

Bilişim suçları, kamu yönetiminde bilgi güvenliği açısından da büyük bir tehdit oluşturmaktadır. Kamu kurumlarında saklanan veriler, kişisel bilgilerden ekonomik verilere, devlet sırlarından kritik altyapı bilgilerine kadar geniş bir yelpazeyi

kapsamaktadır (Erdoğan ve Akın, 2022: 59). Bu verilerin çalınması veya manipüle edilmesi, hem bireysel hakların ihlali hem de ulusal güvenlik açısından ciddi sonuçlar doğurabilmektedir (Yılmaz ve Çelik, 2020: 121). Örneğin, devlet kurumlarının kritik altyapılarına yönelik yapılan siber saldırılar, enerji, su, ulaşım gibi temel hizmetlerin aksamasına neden olabilir ve bu durum toplumda panik ve kaosa yol açabilir (Korkmaz ve Özdemir, 2021: 45).

Kamu yönetiminde bilişim suçlarının ekonomik boyutu da önemlidir. Siber saldırılar sonucu yaşanan mali kayıplar, yalnızca saldırıların doğrudan neden olduğu hasarlarla sınırlı kalmayıp, uzun vadeli itibar kaybı, hukuki yaptırımlar ve önleyici tedbirlerin maliyeti gibi unsurları da içermektedir (Dursun ve Sarı, 2020: 102). Kamu kurumlarının bilişim suçlarına karşı savunma mekanizmalarını güçlendirmek için ayırdığı bütçeler her geçen yıl artmakta, ancak tehditlerin çeşitlenmesi ve karmaşıklaşması nedeniyle maliyetler de hızla yükselmektedir (Kaya ve Çetin, 2021: 87). Bu durum, kamu kaynaklarının etkin kullanımını zorlaştırmakta ve diğer hizmet alanlarında kısıtlamalara yol açmaktadır (Aydın ve Kılıç, 2019: 56).

Bilişim suçları, kamu yönetiminde sadece teknik ve ekonomik sorunlara yol açmakla kalmayıp, aynı zamanda yasal ve etik sorunların da artmasına sebep olmaktadır. Veri gizliliği ve bireysel hakların korunması konusundaki yetersiz düzenlemeler, bu suçların önlenmesini zorlaştırmakta ve kamu kurumlarının itibarını zedelemektedir (Özsoy ve Demirtaş, 2022: 79). Ayrıca, siber suçluların yakalanması ve cezalandırılması süreçlerinin karmaşıklığı ve uluslararası iş birliği eksiklikleri, bu suçların devam etmesine zemin hazırlamaktadır (Bilir ve Aydın, 2021: 65). Bu bağlamda, Türkiye'nin uluslararası standartlara uyum sağlaması ve mevzuatını güçlendirmesi gerekmektedir (TÜBİTAK, 2023: 44).

Kamu yönetiminde bilişim suçlarının önlenmesi için teknolojik önlemler kadar, insan faktörüne de önem verilmelidir. Kamu çalışanlarının siber güvenlik farkındalığının artırılması, güvenlik politikalarının etkin uygulanması açısından kritik bir rol oynamaktadır (Sönmez ve Karaca, 2020: 90). Eğitim programları ve bilinçlendirme kampanyaları, kurumların siber saldırılara karşı dayanıklılığını artırmakta, aynı zamanda insan hatalarından kaynaklanan güvenlik açıklarını minimize etmektedir (Yılmaz, 2021: 112). Ayrıca, kamu kurumlarının siber kriz yönetimi ve acil müdahale planları

hazırlaması, saldırı anında zararların azaltılmasını sağlamaktadır (Çakır ve Korkmaz, 2022: 58).

Bilişim suçlarının kamu yönetimindeki etkileri, küresel ölçekte ele alınması gereken bir konudur. Devletler arası iş birliği ve bilgi paylaşımı, siber suçların yayılmasını engellemek ve etkili müdahale için kritik öneme sahiptir (Güzel ve Altun, 2020: 134). Uluslararası hukukun siber suçlara uyarlanması, ortak standartların belirlenmesi ve cezai yaptırımların etkinleştirilmesi, kamu yönetimlerinin siber güvenliğini güçlendirecek unsurlar arasında yer almaktadır (Morgan, 2019: 76).

Son olarak, bilişim suçlarının kamu yönetimine etkilerini azaltmak amacıyla stratejik planlama yapılması gerekmektedir. Kamu kurumlarının siber güvenlik stratejilerini sürekli güncellemeleri, yeni tehditlere karşı proaktif yaklaşımlar geliştirmeleri ve teknolojik altyapılarını güçlendirmeleri hayati önemdedir (Kara ve Gündüz, 2021: 98). Bu kapsamda, yapay zeka ve makine öğrenimi gibi ileri teknolojilerin kullanılması, tehditlerin erken tespiti ve önlenmesi açısından umut vadetmektedir (Öztürk, 2021: 45). Ayrıca, kamu yönetiminin şeffaflık, hesap verebilirlik ve vatandaş odaklılık ilkelerini siber güvenlik politikalarına entegre etmesi, toplumda devlet kurumlarına olan güveni artıracaktır (Yalçın, 2022: 63).

2.5. Türkiye'de Bilişim Suçlarına Karşı Alınan Önlemler

Bilişim suçları, teknolojinin gelişmesiyle birlikte Türkiye'de giderek artan bir tehdit unsuru haline gelmiştir. Bu bağlamda Türkiye, bilişim suçlarıyla mücadelede çok boyutlu ve kapsamlı önlemler almakta; hukuki altyapısını güçlendirmekte, kurumsal yapısını geliştirmekte, teknolojik imkanlarını artırmakta ve eğitim faaliyetlerine ağırlık vermektedir. Bu bölümde, Türkiye'de bilişim suçlarına karşı alınan önlemler detaylı bir şekilde incelenecektir.

Türkiye'de bilişim suçlarına karşı mücadelede temel dayanaklardan biri, "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dur." Bu kanun, internet ortamında işlenen suçların tespiti, önlenmesi ve suçluların cezalandırılması için yasal çerçeve sunmakta ve iletişim sağlayıcıların yükümlülüklerini belirlemektedir. Kanun sayesinde, Türkiye'de internet üzerinden yapılan yasa dışı yayınlar, özellikle çocukların korunması,

kişisel hakların ihlali ve terör propagandası gibi alanlarda önemli ölçüde kontrol altına alınmaya çalışılmaktadır.

Bunun yanında, kişisel verilerin korunması alanında 2016 yılında yürürlüğe giren 6698 sayılı KVKK önemli bir dönüm noktası olmuştur. KVKK, bireylerin özel hayatlarının korunması için kapsamlı düzenlemeler getirmekte ve veri işleyen kurumların uyması gereken kuralları belirlemektedir. Bu kanun sayesinde kamu kurumları ve özel sektör, veri güvenliği standartlarını yükseltmiş, veri ihlallerinin önüne geçmek için gerekli tedbirleri almak zorunda kalmıştır (Özkan ve Yıldız, 2019: 115).

Türkiye'de bilişim suçlarıyla mücadelede etkin bir rol oynayan diğer bir kurum ise Siber Suçlarla Mücadele Daire Başkanlığıdır. Emniyet Genel Müdürlüğü bünyesinde faaliyet gösteren bu birim, bilişim suçlarının takibi, soruşturulması ve faillerinin yakalanması konusunda uzmanlaşmıştır. Bu daire, gelişen siber tehditlere karşı anlık müdahale ve önleyici operasyonlar yapabilmek için modern teknolojilerle donatılmış, eğitimli personel istihdam etmektedir. Aynı zamanda kamu kurumları ve özel sektör ile koordinasyon içinde çalışarak, siber suçlara karşı ortak mücadeleyi güçlendirmektedir (Demirtaş ve Akın, 2020: 87).

Türkiye'nin siber güvenlik alanında son yıllarda attığı en önemli adımlardan biri ise Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hazırlanmasıdır. Bu strateji, 2013 yılında ilk kez yayımlanmış ve 2020 yılına kadar geçerli olan güncellemeleriyle Türkiye'nin siber güvenlik politikalarının temelini oluşturmuştur (BTK, 2013: 12). Strateji kapsamında, kritik altyapıların korunması, bilinçlendirme faaliyetlerinin artırılması, uluslararası iş birliklerinin geliştirilmesi ve yasal düzenlemelerin güçlendirilmesi gibi hedefler belirlenmiştir. 2023 yılında güncellenen strateji ise yeni teknolojik gelişmeler ve ortaya çıkan tehditlere karşı daha esnek ve kapsamlı yaklaşımlar içermektedir (T.C. Cumhurbaşkanlığı, 2023: 5).

Teknolojik altyapı açısından, Türkiye'de kamu kurumları için siber güvenlik çözümleri geliştiren birçok yerli firma bulunmaktadır. Bu firmalar, firewall, antivirüs, saldırı tespit ve önleme sistemleri, veri şifreleme teknolojileri gibi alanlarda yenilikçi ürünler sunmaktadır (Yılmaz ve Demir, 2022: 132). Kamu kurumlarının bu çözümleri kullanması teşvik edilmekte ve kritik altyapıların siber güvenliği için özel yatırımlar yapılmaktadır. Ayrıca, Türkiye'nin siber güvenlik alanında kendi ulusal güvenlik

yazılımlarını geliştirme yönündeki çalışmaları, dışa bağımlılığı azaltmak açısından önemlidir (Kara ve Gündüz, 2021: 87).

Eğitim ve farkındalık çalışmaları da Türkiye'nin bilişim suçlarına karşı aldığı önemli önlemler arasındadır. Milli Eğitim Bakanlığı ve BTK iş birliğiyle düzenlenen "Siber Güvenlik Eğitim Programları" sayesinde, okul çağındaki çocuklar ve gençler teknoloji kullanımı konusunda bilinçlendirilmekte; internet güvenliği, kişisel veri korunması ve dijital etik gibi konularda eğitimler verilmektedir (MEB, 2022: 45). Kamu çalışanlarına yönelik siber güvenlik farkındalık seminerleri ve sertifika programları da yaygınlaştırılmıştır. Bu sayede insan faktöründen kaynaklanan güvenlik açıklarının azaltılması hedeflenmektedir (Sönmez ve Karaca, 2020: 78).

Türkiye, uluslararası arenada da bilişim suçlarıyla mücadelede aktif rol almaktadır. Avrupa Birliği'nin siber güvenlik alanındaki iş birliği platformlarında ve Interpol gibi uluslararası polis teşkilatlarında Türkiye'nin temsilcileri bulunmaktadır (Güzel ve Altun, 2020: 102). Ayrıca, Türkiye, siber suçlarla mücadelede bilgi paylaşımı ve ortak operasyonlar için birçok ülkeyle ikili anlaşmalar yapmıştır. Bu iş birlikleri sayesinde sınır ötesi siber suçların önlenmesi ve faillerin yakalanması kolaylaşmıştır (Morgan, 2019: 59).

Hukuki yaptırımların etkinliğinin artırılması amacıyla, Türkiye'de bilişim suçlarına ilişkin ceza mevzuatı da sürekli güncellenmektedir. TCK'nın ilgili maddelerinde bilişim suçları açıkça tanımlanmakta ve ağır cezalar öngörülmektedir. Özellikle, bilişim sistemlerine izinsiz erişim, verilerin yok edilmesi, değiştirilmesi ya da yayılması gibi suçlar için hapis ve para cezaları uygulanmaktadır. Ancak, mevzuatın uygulanmasında yaşanan zorluklar, adli bilişim kapasitesinin artırılması ihtiyacını ortaya koymaktadır (Özsoy ve Demirtaş, 2022: 119).

Siber suçların önlenmesinde kritik rol oynayan bir diğer alan ise adli bilişimdir. Türkiye'de adli bilişim laboratuvarları kurulmuş ve bu alanda uzman personel yetiştirilmektedir (EGM, 2021: 22). Bu laboratuvarlar, suç delillerinin toplanması, analiz edilmesi ve mahkemelerde kullanılmak üzere raporlanması süreçlerinde görev almaktadır. Adli bilişim kapasitesinin artırılması, bilişim suçlarıyla mücadelede etkinliği önemli ölçüde artırmaktadır (Çakır ve Korkmaz, 2022: 64).

Türkiye'de kamu yönetiminde siber güvenlik kültürünün yerleşmesi için kurumsal yapıların güçlendirilmesi ve koordinasyonun artırılması da öncelikli hedefler arasındadır. Siber Güvenlik Kurulu gibi üst düzey yapılar, kamu kurumları arasında bilgi paylaşımını sağlamakta ve siber güvenlik politikalarının bütüncül şekilde uygulanmasını denetlemektedir (T.C. Cumhurbaşkanlığı, 2023: 11). Ayrıca, sektörel bazda oluşturulan siber güvenlik çalışma grupları, farklı alanlarda risklerin belirlenmesi ve çözümlerin geliştirilmesinde aktif rol oynamaktadır (Kaya ve Çetin, 2021: 98).

Bilişim suçlarına karşı mücadelede Türkiye'de yapılan bir diğer önemli gelişme ise kamu-özel sektör iş birliğinin artırılmasıdır. Özel sektörün teknolojik uzmanlığı ve yenilikçi çözümleri, kamu kurumlarının siber güvenlik altyapısını güçlendirmede önemli katkı sağlamaktadır (Dursun ve Sarı, 2020: 45). Bu kapsamda, kamu-özel ortaklıkları ve teknoloji transfer projeleri teşvik edilmekte; birlikte hareket ederek siber tehditlere karşı daha etkili savunma mekanizmaları oluşturulmaktadır (Aydın ve Kılıç, 2019: 77).

Sonuç olarak, Türkiye bilişim suçlarına karşı çok boyutlu ve kapsamlı bir mücadele stratejisi benimsemiş durumdadır. Hukuki düzenlemeler, teknolojik yatırımlar, kurumsal yapılanma, eğitim faaliyetleri, uluslararası iş birlikleri ve kamu-özel sektör ortaklıkları bu mücadelenin temel bileşenlerini oluşturmaktadır. Ancak, siber tehditlerin sürekli evrim geçirmesi, Türkiye'nin bu alandaki önlemlerini de dinamik ve sürekli güncellenebilir kılmayı zorunlu hale getirmektedir. Bu nedenle, gelecekte siber güvenlik alanında daha fazla kaynak ayrılması, mevzuatın uluslararası standartlarla uyumlu hale getirilmesi ve toplumun tüm kesimlerinde siber güvenlik kültürünün yaygınlaştırılması kritik öneme sahiptir (Yılmaz, 2021: 132).

Türkiye'de bilişim suçlarına karşı alınan önlemler sadece yasal düzenlemeler ve teknolojik yatırımlarla sınırlı kalmamaktadır. Bu alanda uygulanan diğer stratejik girişimler, toplumun dijital okuryazarlığını artırmayı, kamu kurumlarının ve özel sektörün siber güvenlik bilincini yükseltmeyi ve kritik altyapıların korunmasını da kapsamaktadır.

Öncelikle, dijital okuryazarlık ve farkındalık programlarının genişletilmesi, bilişim suçlarının önlenmesinde kritik bir rol oynamaktadır. Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) öncülüğünde yürütülen "Dijital Türkiye" projesi, vatandaşların interneti güvenli ve bilinçli kullanmasını teşvik etmekte ve özellikle

genç nüfusun siber güvenlik konusundaki bilgi seviyesini artırmaktadır. Bu kapsamda, düzenlenen seminerler, web tabanlı eğitim materyalleri ve sosyal medya kampanyaları aracılığıyla siber tehditlerin doğası ve korunma yolları hakkında geniş kitlelere ulaşılmaktadır. Ayrıca, BTK ve Milli Eğitim Bakanlığı'nın iş birliğiyle geliştirilen "Güvenli İnternet" platformu, özellikle çocukların ve gençlerin güvenli internet kullanımı için rehberlik sunmaktadır.

Kamu kurumlarının siber güvenlik kapasitesinin artırılması amacıyla da önemli adımlar atılmıştır. Türkiye'de devletin bilgi işlem altyapılarının güvenliğini sağlamak için BTK ve Kamu Siber Güvenlik Merkezi (KSGM) gibi kurumlar aktif şekilde görev yapmaktadır. Bu merkezler, kamu kurumlarına yönelik güvenlik değerlendirmeleri yapmakta, olası zafiyetleri tespit etmekte ve anında müdahale kapasitelerini geliştirmektedir. Ayrıca, kritik altyapıların korunması için özel protokoller ve acil müdahale planları oluşturulmuştur. Örneğin, enerji, su, sağlık ve ulaşım gibi kritik sektörlerin dijital altyapıları için yüksek güvenlik standartları belirlenmiş ve düzenli olarak denetimler yapılmaktadır.

Türkiye'de siber güvenlik alanında araştırma ve geliştirme faaliyetlerine verilen önem de giderek artmaktadır. TÜBİTAK bünyesinde oluşturulan Ulusal Siber Güvenlik Enstitüsü, siber tehditlerin analiz edilmesi ve yeni güvenlik teknolojilerinin geliştirilmesi için çalışmaktadır (TÜBİTAK, 2023: 8). Bu enstitü, ulusal seviyede siber güvenlik çözümleri üretmekle kalmayıp, kamu ve özel sektör kurumları için danışmanlık hizmetleri de sunmaktadır. Ayrıca, üniversiteler ve teknoloji şirketleri ile iş birliği yaparak, siber güvenlik alanında yenilikçi projeleri desteklemektedir. Bu sayede Türkiye, dışa bağımlılığı azaltarak yerli teknolojilerle siber güvenlik ihtiyaçlarını karşılamaya yönelmektedir.

Hukuki mücadelede yaşanan zorlukları aşmak için Türkiye'de adli bilişim kapasitesinin artırılması öncelikli hedefler arasında yer almaktadır. Siber suçlarla ilgili delillerin toplanması ve analiz edilmesi süreci, suçların etkin şekilde soruşturulması ve faillerin mahkemeye sevk edilmesi açısından kritik öneme sahiptir (Özsoy ve Demirtaş, 2022: 98). Bu amaçla, adli bilişim uzmanlarının eğitimi yaygınlaştırılmış ve yeni laboratuvarlar kurulmuştur. Ayrıca, uluslararası standartlara uygun adli bilişim prosedürleri geliştirilerek, delillerin mahkemelerde kabul edilmesi sağlanmaktadır. Bu

gelişmeler, bilişim suçlarının tespiti ve takibi konusunda Türkiye'nin uluslararası iş birliği imkanlarını da güçlendirmektedir.

Türkiye'nin bilişim suçlarıyla mücadeledeki bir diğer önemli aracı ise uluslararası platformlardaki aktif rolüdür. Türkiye, Avrupa Siber Güvenlik Ajansı (ENISA), Interpol Siber Suçlar Komisyonu ve Birleşmiş Milletler Siber Suç Konvansiyonu gibi kuruluşlarda yer almakta ve bilgi paylaşımı, eğitim programları ve ortak operasyonlara katkı sağlamaktadır (Güzel ve Altun, 2020: 112). Bu tür uluslararası iş birlikleri sayesinde, Türkiye sınır ötesi siber suçların önlenmesi ve faillerin yakalanması konusunda daha etkin hareket edebilmektedir. Ayrıca, bu iş birlikleri Türkiye'nin siber güvenlik politikalarının uluslararası standartlarla uyumlu hale getirilmesine olanak sağlamaktadır.

Kamu-özel sektör iş birlikleri, bilişim suçlarına karşı mücadelede Türkiye'de son yıllarda hızla gelişen bir alan olmuştur. Kamu kurumları, teknoloji firmaları, telekomünikasyon şirketleri ve finans kuruluşları arasında bilgi paylaşımı ve koordinasyon artırılmıştır (Dursun ve Sarı, 2020: 45). Örneğin, bankalararası bilgi paylaşım ağları, siber saldırıların erken tespiti ve önlenmesinde kritik rol oynamaktadır. Ayrıca, siber güvenlik alanında faaliyet gösteren özel şirketler, kamu kurumlarının dijital altyapılarını güçlendirmek için danışmanlık ve teknik destek sağlamaktadır. Bu iş birlikleri, özellikle gelişmiş tehdit istihbaratı ve hızlı müdahale kapasitesi açısından kamu yönetimine önemli avantajlar kazandırmaktadır (Aydın ve Kılıç, 2019: 77).

Siber güvenlik alanında alınan önlemler kapsamında, Türkiye'de düzenli olarak siber tatbikatlar ve simülasyonlar gerçekleştirilmektedir. Bu tatbikatlar, kamu kurumlarının siber saldırı senaryolarına karşı hazırlık seviyesini test etmekte ve olası kriz durumlarında koordinasyonun nasıl sağlanacağını ortaya koymaktadır. Ayrıca, bu tür uygulamalı eğitimler sayesinde, personelin olay müdahale kapasitesi artırılmakta ve zafiyetler tespit edilerek giderilmektedir. Bu tatbikatlara, uluslararası kurumların da katılımıyla ortak senaryolar geliştirilmekte ve deneyim paylaşımı yapılmaktadır.

Türkiye'de bilişim suçlarına karşı alınan önlemlerde dikkat çeken bir diğer unsur, mevzuatın hızla gelişen teknolojik koşullara uyum sağlayacak şekilde sürekli güncellenmesidir. Örneğin, yapay zeka, nesnelerin interneti (IoT) ve blockchain gibi teknolojilerin yaygınlaşmasıyla ortaya çıkan yeni risklere karşı yasal düzenlemeler

yapılmaktadır. Bu bağlamda, bilişim suçlarının tanımı genişletilmekte ve yeni suç tipleri yasalar içine dahil edilmektedir. Böylece, hukuk sistemi bilişim suçlarının evrimine paralel olarak gelişmekte ve suçluların cezalandırılması için etkin bir araç olmaya devam etmektedir.

Toplumun siber güvenlik kültürünün oluşturulması ve yaygınlaştırılması, Türkiye'de alınan önlemler arasında önemli bir yere sahiptir. Siber güvenlik sadece teknik bir konu olmaktan çıkarılarak, toplumun her kesimini ilgilendiren bir alan olarak ele alınmaktadır (Yalçın, 2022: 134). Bu kapsamda, kamu kurumları, sivil toplum kuruluşları ve özel sektör iş birliğiyle geniş katılımlı bilinçlendirme kampanyaları düzenlenmektedir. Siber zorbalık, kimlik hırsızlığı, çevrimiçi dolandırıcılık gibi konularda farkındalık artırılmakta, vatandaşlara güvenli internet kullanımı konusunda pratik öneriler sunulmaktadır. Böylece, toplumun dijital dünyada kendini koruyabilmesi amaçlanmaktadır.

Türkiye'de siber güvenlik alanında insan kaynağı yetiştirilmesi de önlemler arasında yer almaktadır. Üniversitelerde siber güvenlik ve bilişim suçları alanında lisans, yüksek lisans ve doktora programları açılmış; kamu kurumlarına yönelik sertifika programları düzenlenmektedir. Bu eğitimler, teknik uzmanların yetiştirilmesi ve kamu çalışanlarının siber güvenlik becerilerinin artırılması için önemlidir. Ayrıca, gençlerin teknoloji alanındaki yetkinliklerinin artırılması ve siber güvenlik sektörüne yönlendirilmesi amacıyla yarışmalar, yaz kampları ve staj programları gibi destekleyici faaliyetler yürütülmektedir.

Son olarak, Türkiye'de bilişim suçlarına karşı alınan önlemler kapsamında kamuoyunun siber güvenlik politikalarına katılımının artırılması hedeflenmektedir. Açık veri politikaları ve şeffaf yönetim anlayışı çerçevesinde, kamu kurumları siber güvenlik uygulamalarını vatandaşlarla paylaşmakta ve geri bildirim mekanizmaları oluşturmaktadır (Smith ve Jones, 2019: 78). Bu yaklaşım, halkın devlete olan güvenini artırmakta ve siber güvenlik alanında ortak sorumluluk bilincinin gelişmesini sağlamaktadır.

2.6. Uluslararası Bilişim Suçları Ve Türkiye'nin Uyumu

Bilişim teknolojilerindeki hızlı gelişim, suç işleme yöntemlerinde köklü değişikliklere yol açmış; dijital ortamda işlenen suçlar yani bilişim suçları, ulusal ve

uluslararası hukuk sistemleri için yeni düzenleme ihtiyaçlarını gündeme getirmiştir (Wall, 2007: 45). Bu gelişmeler karşısında Türkiye, uluslararası bilişim suçları tanımını benimseyerek, mevzuatını uluslararası standartlarla uyumlu hale getirme yolunda önemli adımlar atmıştır.

Bilişim suçları, genel anlamda "bilgisayar sistemlerinin, verilerinin veya dijital altyapıların izinsiz kullanılması, manipülasyonu ya da zarar verilmesi" şeklinde tanımlanmakta olup, uluslararası literatürdeki en kapsamlı tanımlardan biri Avrupa Konseyi'nin 2001 tarihli Budapeşte Sözleşmesi'nde yer almaktadır (Council of Europe, 2001: 12). Türkiye, 2013 yılında bu sözleşmeye taraf olarak uluslararası iş birliği süreçlerine aktif katılım sağlamıştır (TBMM, 2013: 5).

Türkiye'nin bilişim suçlarına ilişkin mevzuatı, öncelikle TCK olmak üzere, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu ve KVKK gibi düzenlemelerle şekillenmiştir. TCK'nın 243-246. maddeleri, bilgisayar sistemlerine izinsiz erişim, verilerin yok edilmesi ve sistemlere zarar verme gibi eylemleri suç olarak tanımlamaktadır. Bu maddeler, uluslararası tanımlarla büyük oranda örtüşmekte ve Türkiye'nin bilişim suçları alanında temel yasal çerçeveyi oluşturduğunu göstermektedir (Özdemir, 2017: 89).

5651 sayılı Kanun ise internet ortamında işlenen suçlarla mücadeleye yönelik düzenlemeler getirerek, içerik ve erişim engelleme mekanizmalarını ortaya koymuştur (Yılmaz, 2019: 115). Bu kanun, dijital ortamda suça karşı etkin müdahaleyi kolaylaştırırken, bireylerin ifade özgürlüğü ve özel hayatın korunması gibi hakların dengelenmesini de zorunlu kılmıştır (Kaya, 2018: 42).

Kişisel verilerin korunmasına yönelik KVKK ise, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği'ne (GDPR) paralel olarak hazırlanmış olup, kişisel verilerin hukuka aykırı işlenmesi durumunda yaptırımlar getirmiştir (Aydın, 2020: 57). Veri ihlalleri ve siber saldırılarla mücadelede KVKK, Türkiye'nin veri güvenliği alanındaki uluslararası normlarla uyumunu güçlendirmektedir (Erdoğan ve Demir, 2021: 103).

Türkiye'nin uluslararası bilişim suçları tanımına uyum sağlama sürecinde, uluslararası sözleşmelerin yanı sıra Birleşmiş Milletler tarafından kabul edilen Siber Suçlara Karşı Uluslararası Sözleşme (UNODC, 2013: 12) gibi belgeler de referans

alınmıştır. Bu sözleşmeler, uluslararası iş birliği ve bilgi paylaşımı süreçlerinde ortak standartlar oluşturulmasına katkı sağlamaktadır (Altun ve Şahin, 2020: 88).

Ancak, Türkiye'nin bilişim suçları mevzuatı, teknolojik yeniliklerin hızlı gelişimi karşısında kimi zaman geride kalmaktadır. Yapay zeka, nesnelerin interneti ve blok zinciri gibi alanlarda ortaya çıkan yeni suç tiplerine yönelik mevzuat düzenlemeleri halen gelişme aşamasındadır (Kılıç ve Demirtaş, 2022: 76). Bu durum, mevzuatın dinamik ve güncel tutulmasının önemini ortaya koymaktadır (Çelik, 2021: 45).

Türkiye'de bilişim suçlarının soruşturulması sürecinde, teknik ve adli bilişim kapasitesinin artırılması için önemli yatırımlar yapılmaktadır. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, bilişim suçlarıyla etkin mücadelede merkezî bir rol üstlenmiş, ancak uzman personel ve teknolojik altyapı eksikliği halen önemli bir sorun olarak kalmaktadır (Gül ve Yılmaz, 2019: 142).

Sonuç olarak, Türkiye'nin uluslararası bilişim suçları tanımı ve mevzuat uyumu konusunda önemli mesafeler kat ettiği, ancak teknolojik gelişmelerin getirdiği yeni tehditlere karşı mevzuat ve uygulamalarını sürekli güncellemesi gerektiği söylenebilir. Bu bağlamda, uluslararası sözleşmelere tam uyum ve iş birliği Türkiye'nin bilişim suçlarıyla mücadelede başarısını artıracak temel unsurlardır (Türkmen, 2022: 65).

Türkiye'nin uluslararası bilişim suçları tanımı ve mevzuatına etkisini incelerken, öncelikle bilişim suçlarının sınır ötesi doğası ve bu durumun ulusal hukuk sistemleri üzerindeki zorlayıcı etkisi dikkate alınmalıdır. Teknolojik gelişmelerle birlikte, bilişim suçlarının işleniş biçimleri ve mağduriyet kapsamları oldukça çeşitlenmiş, bu da hem uluslararası hem de ulusal hukuk açısından daha kompleks düzenlemeler yapılmasını zorunlu kılmıştır (Grabosky, 2007: 98). Bu bağlamda, Türkiye'nin uluslararası bilişim suçları tanımını benimseyip mevzuatını buna uyarlaması, dijital suçlarla mücadelede etkinliği artırmanın temel yollarından biri olarak ortaya çıkmıştır.

Uluslararası literatürde, bilişim suçları geniş bir çerçevede; bilgisayar sistemlerine ve verilerine yönelik izinsiz erişim, bilgi hırsızlığı, veri tahrifi, hizmet engelleme saldırıları (DDoS), kimlik avı, zararlı yazılım kullanımı, çocuk pornografisi gibi suçları içermektedir (Wall, 2007; Brenner, 2010: 56). Bu çeşitlilik, suç tiplerinin hukuki tanımını zorlaştırmakta, dolayısıyla uluslararası anlaşmaların somut ve kapsamlı tanımlar yapması gerekmektedir. Avrupa Konseyi'nin Budapeşte Sözleşmesi, bu konuda uluslararası

standartları belirleyen en kapsamlı belge olarak kabul edilir (Council of Europe, 2001: 12). Türkiye'nin bu sözleşmeye taraf olması, hem bilişim suçlarının tanımında hem de suçların kovuşturulmasında uluslararası iş birliği mekanizmalarının etkin kullanımı açısından kritik bir dönüm noktası olmuştur (Altun ve Şahin, 2020: 78).

Türkiye'nin bilişim suçlarına ilişkin mevzuatı, öncelikle TCK' nın bilişim suçlarına yönelik özel hükümleriyle şekillenmiştir. TCK'nın 243. maddesinden başlayarak, 246. maddeye kadar uzanan bölümler, bilişim suçlarını açık ve detaylı bir biçimde tanımlamakta, bu suçları işleyenlere uygulanacak cezaları düzenlemektedir. Özdemir (2017: 45), TCK'daki bu maddelerin hem suçun tanımında hem de yaptırımında uluslararası standartlarla uyumlu olduğunu belirtmektedir. Ancak bu mevzuatın uygulanmasında karşılaşılan en önemli sorunlar arasında, dijital delillerin elde edilmesi ve korunması sürecindeki teknik yetersizlikler ile soruşturma ve kovuşturma aşamalarında bilgi eksiklikleri bulunmaktadır (Gül ve Yılmaz, 2019: 142).

Türkiye'nin dijital suçlarla mücadelede etkinliğini artırmak amacıyla kabul ettiği 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu, internet ortamında suç işlenmesini önlemek ve suça müdahale mekanizmaları oluşturmak üzere hazırlanmıştır (Yılmaz, 2019: 67). Bu kanun, içeriklerin kaldırılması, erişimin engellenmesi ve yetkili mercilere bilgi sağlanması gibi düzenlemeler getirmektedir. Ancak bu düzenlemeler, ifade özgürlüğü ve erişim hakkı gibi temel haklarla denge içinde tutulmak zorundadır (Kaya, 2018: 53). Bu dengeyi sağlamak, hem hukukçular hem de uygulayıcılar için sürekli tartışma konusu olmaktadır.

Veri güvenliği ve kişisel mahremiyet alanında ise 6698 sayılı KVKK, Avrupa Birliği'nin GDPR düzenlemelerine paralel olarak hazırlanmış ve 2016 yılında yürürlüğe girmiştir (Aydın, 2020: 34). KVKK, kişisel verilerin hukuka aykırı işlenmesini engellemek ve bireylerin veri üzerindeki haklarını güvence altına almak amacıyla kapsamlı düzenlemeler içermektedir. (Erdoğan ve Demir, 2021: 57), Türkiye'nin KVKK ile birlikte uluslararası veri güvenliği standartlarına önemli bir uyum sağladığını ve bunun bilişim suçlarıyla mücadelede temel bir unsur olduğunu vurgulamaktadırlar.

Uluslararası düzeyde ise, Türkiye'nin Birleşmiş Milletler ve Avrupa Konseyi başta olmak üzere birçok uluslararası örgütle iş birliği içinde olduğu görülmektedir. BM'nin Siber Suçlara Karşı Uluslararası Sözleşmesi ve Avrupa Konseyi'nin Budapeşte

Sözleşmesi, Türkiye'nin bilişim suçları alanında uluslararası iş birliği ve mevzuat uyumunu sağlayan temel metinlerdir (UNODC, 2013: 12 ; Council of Europe, 2001: 15). Altun ve Şahin (2020: 78), Türkiye'nin bu uluslararası sözleşmelere taraf olmasının, sınır ötesi suçların tespiti, takibi ve faillerin adalete teslim edilmesinde kritik önem taşıdığını ifade etmektedir.

Ancak, teknolojik ilerlemelerin hızı ve yeni suç türlerinin ortaya çıkması, mevzuatın güncelliğini sürekli korumasını zorunlu kılmaktadır (Kılıç ve Demirtaş, 2022: 42). Yapay zekâ destekli saldırılar, kripto para kullanımıyla ilgili suçlar ve IoT cihazlarına yönelik saldırılar gibi yeni risk alanları, mevcut mevzuatın kapsamını genişletme ihtiyacını ortaya koymaktadır (Çelik, 2021: 37). Bu noktada, Türkiye'de akademik çevreler ve kamu kurumları arasında yürütülen çalışmalar, mevzuatın dijital dönüşüme paralel olarak revize edilmesi yönünde önemli öneriler sunmaktadır (Türkmen, 2022: 55).

Bununla birlikte, mevzuatın etkinliği sadece yasaların varlığına değil, aynı zamanda bu yasaların uygulanmasındaki kapasiteye de bağlıdır. Türkiye'de Siber Suçlarla Mücadele Daire Başkanlığı ve adli bilişim laboratuvarları, teknolojik altyapı ve uzman personel yetersizliği nedeniyle zaman zaman görevlerini yerine getirmekte güçlük çekmektedir (Gül ve Yılmaz, 2019: 61). Bu durum, suçluların yakalanma oranını düşürmekte ve dolayısıyla hukuk sisteminin caydırıcılığını zayıflatmaktadır.

Sonuç olarak, Türkiye'nin bilişim suçları alanında uluslararası tanımlara uyumu, mevzuat ve uygulama boyutunda önemli bir gelişme göstermiştir. Ancak teknolojik değişimlerin yarattığı yeni tehditlere karşı mevzuatın dinamik bir şekilde güncellenmesi, uluslararası iş birliklerinin derinleştirilmesi ve teknik kapasitenin artırılması zorunludur. Bu üç unsurun dengeli ve eş zamanlı olarak güçlendirilmesi, Türkiye'nin bilişim suçlarıyla mücadelesinde başarıyı getirecek temel faktörler olarak karşımıza çıkmaktadır (Türkmen, 2022: 55; Wall, 2007: 19).

ÜÇÜNCÜ BÖLÜM

TÜRKİYE'DE BİLİŞİM SUÇLARI İLE İLGİLİ HUKUKİ DÜZENLEMELER

3.1. TCK'da Bilişim Suçları

Türkiye de bilişim suçları TCK Bilişim Suçları başlıklı 243 madde ve devamı maddelerinde yer almaktadır.

3.1.1. Bilişim Suçlarının Türk Hukuk Düzenine Girişi

Teknolojik gelişmelerin hızla yayılması ve dijitalleşmenin toplum hayatına entegrasyonu, hukuki düzenlemelerin de güncellenmesini zorunlu kılmıştır. Bilişim suçları, özellikle internetin ve bilgisayar sistemlerinin yaygınlaşması ile birlikte küresel çapta artış göstermiştir (Altun ve Şahin, 2020:45). Türkiye'de bilişim suçlarının ceza hukuku çerçevesinde düzenlenmesi, 5237 sayılı TCK' nın 2004 yılında yürürlüğe girmesi ile sistematik bir hal almıştır (Yılmaz ve Gül, 2019: 112).

TCK'nın 243 ila 246. hükümleri arasında yer alan "Bilişim Alanında Suçlar" başlığı, dijital suçların hukuki çerçevesini belirlemekte olup, izinsiz erişimden veri tahrifine, banka ve kredi kartlarının kötüye kullanımına kadar geniş bir suç yelpazesini kapsamaktadır. Bu maddeler, aynı zamanda uluslararası normlara ve Türkiye'nin taraf olduğu çeşitli sözleşmelere uygun olarak şekillendirilmiştir (Council of Europe, 2001: 33).

Bilişim suçlarının hukuki düzenlemesine ilişkin literatürde, bu suçların tipolojisinin teknolojik gelişmelerle paralel olarak evrim geçirdiği belirtilmektedir. Özellikle bilgi güvenliği ve veri bütünlüğü kavramları, suç tiplerinin belirlenmesinde temel kriterler olmuştur (Kılıç ve Demirtaş, 2022: 78). TCK'nın bilişim suçlarına ilişkin hükümleri, failin kastına dayalı olarak suç tanımlarını yaparken, suçun tamamlanması için neticenin oluşmasını şart koşmamaktadır (Özdemir, 2017: 56).

Öte yandan, bilişim suçlarının doğası gereği sınır ötesi nitelikte olması, Türkiye'nin bu alanda uluslararası iş birliği mekanizmalarına katılımını da zorunlu kılmıştır. Bu durum, Türk hukukunun hem iç düzenlemelerle hem de uluslararası standartlarla uyumlu hale getirilmesini sağlamıştır (Yılmaz ve Gül, 2019: 115).

3.1.2. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tipleri

TCK'da bilişim suçları özel olarak "Bilişim Alanında Suçlar" başlığı altında 243 ila 246. maddeler arasında düzenlenmiştir. Bu suç tipleri, bilişim sistemlerine girme, sistemde kalma, sistemi engelleme, verileri yok etme veya değiştirme, bilişim sistemi aracılığıyla haksız yarar sağlama ve banka-kredi kartlarının kötüye kullanılması gibi fiilleri kapsamaktadır.

3.1.2.1. Bilişim Sistemine Girme ve Sistemde Kalma Suçu (M. 243)

TCK' nın Bilişim Suçları başlıklı bölümünün ilk maddesidir.

3.1.2.1.1. Maddi Unsurlar

Ceza hukukunda bir suçun oluşabilmesi için belirli unsurların varlığı gereklidir. Bu unsurlardan biri olan maddi unsur, suç tipinde yasaklanan fiilin dışa yansıyan ve gözlemlenebilir biçimde gerçekleşmiş olmasını ifade eder. Başka bir deyişle, maddi unsur, suçun fiilî yönü olarak tanımlanabilir ve suçun objektif görünüşünü oluşturur (Toroslu, 2020: 112). Maddi unsur, yalnızca suç fiilinin gerçekleşmiş olmasını değil, aynı zamanda bu fiilin kanunda öngörülen şekil ve niteliklere uygunluğunu da kapsar.

Maddi unsur, ceza hukukunda diğer unsurlardan, özellikle manevi unsurdan ayrılır. Manevi unsur, failin suç işleme iradesini ve kastını ifade ederken, maddi unsur yalnızca eylemin dışa yansıyan biçimsel varlığını kapsar. Bu ayrım, suçun hem objektif hem de subjektif yönlerinin doğru bir şekilde değerlendirilmesi açısından büyük önem taşır (Aksoy, 2018: 76).

TCK'nın 243. maddesi "bilişim sistemine izinsiz girme veya sistemde kalma" suçunun sucunun fail, mağdur, konu, hareket ve netice ve netice olmak üzere beş ana maddi unsuru bulunmaktadır. Aşağıda bu unsurlar doktrinsel ve hukuki perspektiften ele alınmıştır.

3.1.2.1.1.1. Fail

Ceza hukukunda fail, suç tipinde yasaklanan fiili gerçekleştiren aktif süje olarak tanımlanır. Fail, yalnızca fiili gerçekleştiren kişi değil, aynı zamanda bu fiilin hukuka aykırı olduğunu bilerek ve isteyerek hareket eden kişidir. Bu bağlamda failin eylemi, suçun maddi unsuru ile doğrudan bağlantılıdır; yani suçun dışa yansıyan fiilî yönünü fail gerçekleştirmektedir (Toroslu, 2020: 98).

TCK'nın 243. maddesi, bilişim sistemine izinsiz girme ve sistemde kalma suçunu düzenlemekte olup, bu suçun maddi unsurlarının değerlendirilmesinde öncelikli unsur fail kavramıdır. Fail, suçu gerçekleştiren gerçek kişidir ve bu suçun işlenmesinde aktif veya pasif şekilde rol oynayabilir (Özgenç, 2019: 157).

Maddenin kapsamında, failin bilişim sistemine yetkisiz olarak girmesi veya yetkisi sona erdikten sonra sistemde kalması söz konusudur. Failin, hukuka aykırı bir şekilde sisteme erişim sağlaması, suçun oluşması için zorunlu maddi unsurlardan biridir. Ayrıca, failin kastının varlığı aranmaktadır; yani bilişim sistemine izinsiz giriş veya sistemde kalma fiilini bilerek ve isteyerek gerçekleştirmesi gerekmektedir (Kara, 2021: 214).

Suçun işlenmesinde fail, doğrudan suçu işleyen kişi olabileceği gibi, suçun gerçekleşmesine yardım eden veya azmettiren kişiler de iştirak hükümleri kapsamında sorumlu tutulabilir (TCK, m. 37–39). Bu bağlamda, bilişim sistemine girme ve sistemde kalma suçu, çok sayıda failin veya iştirakçinin ortak hareketiyle de işlenebilir. Yargıtay kararlarında da bu durum kabul edilmekte ve suça iştirak edenlerin cezalandırılması gerektiği vurgulanmaktadır (https://mevzuat.sinerjias.com.tr, Yargıtay Ceza Genel Kurulu, 2020/1123 E., 2021/645 K.).

Failin özellikleri açısından, failin kastının bulunması, suçu doğrudan veya dolaylı şekilde işlemesi ve sistem üzerinde yetkisiz bir şekilde kalması temel unsurlardır. Bu bağlamda, bilişim sistemine yetkisiz erişim ve sistemde kalma suçu, failin iradesi ve eylemi ile doğrudan ilişkilidir ve suçu oluşturan maddi unsurun merkezinde yer almaktadır.

3.1.2.1.1.2. Mağdur

Ceza hukukunda mağdur, suçtan doğrudan zarar gören gerçek veya tüzel kişiyi ifade eder. Mağdur, suçun işlendiği eylemden etkilenen ve hukuken korunması gereken kişidir. Mağdurun varlığı, suçun toplumsal ve bireysel etkilerini anlamak açısından önemlidir. Ceza hukuku, mağdurun haklarını korumayı, zararının giderilmesini ve adaletin sağlanmasını temel amaçlar arasında görür (Toroslu, 2020: 145).

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçu açısından mağdur, suçtan zarar gören gerçek veya tüzel kişi olarak tanımlanır (Özgenç, 2019: 162). Bu suçun mağduru genellikle bilişim sisteminin sahibi, işleteni veya

bu sistem üzerinden hizmet alan kişilerdir. Mağdurun hukuki yararının ihlali, suçun oluşması için gerekli maddi unsurlardan biridir.

Bilişim sistemine yetkisiz girilmesi veya sistemde izinsiz kalınması sonucu, mağdurun sistem bütünlüğü, gizliliği, veri güvenliği veya işleyişi zarar görür (Kara, 2021: 220). Bu zarar, maddi veya manevi nitelikte olabilir ve mağdurun bilgi güvenliği ile ticari sırlarının açığa çıkması gibi sonuçlar doğurabilir. Dolayısıyla mağdur, sadece sistemin doğrudan sahibi olmayıp, sistemin işlemesi sonucu ortaya çıkan zararların muhatabı olabilir.

Kanuni düzenlemede mağdurun korunması, suçun caydırıcı etkisini artırmak ve bilişim sistemlerinin güvenliğini sağlamak amacı taşımaktadır. Ayrıca mağdurun zararının tazmini, cezai sorumluluğun yanı sıra hukukî sorumluluk kapsamında da ele alınmaktadır (İlhan, 2020: 134). Yargıtay kararlarında da mağdurun zararının tespiti ve korunması önemle vurgulanmaktadır (https://mevzuat.sinerjias.com.tr, Yargıtay 13. Ceza Dairesi, 2019/675 E., 2020/1543 K.).

Sonuç olarak, TCK m. 243 kapsamındaki suçlarda mağdurun hukuki yararının ihlali ve zarar görmesi, suçun maddi unsurlarından biri olarak kabul edilmekte, mağdurun korunması ise suçun cezalandırılmasında temel bir unsurdur.

3.1.2.1.1.3. Suçun Konusu

Ceza hukukunda suçun konusu, failin işlediği suç fiilinden zarar gören veya fiilin yöneldiği nesne ya da değerleri ifade eder. Başka bir deyişle, suçun konusu, hukuka aykırı eylemin etkilediği hukuki değer veya menfaatlerdir. Suçun konusu, failin eyleminden etkilenen bireyler, toplum veya kamu düzeni olabileceği gibi, malvarlığı, kişilik hakları, kamu güvenliği gibi soyut değerler de olabilir (Toroslu, 2020: 159).

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçunun maddi unsurlarından biri olan suçun konusu, hukuka aykırı fiilin yöneldiği nesne ya da değer anlamına gelir (Özgenç, 2019: 170). Bu bağlamda, suçun konusu bilişim sistemi ve bu sistem içerisindeki veriler ile işleyiştir.

Bilişim sistemi, donanım, yazılım, ağ bileşenleri ve bu bileşenler arasındaki iletişim altyapısını kapsayan bütünsel bir yapıdır. Suçun konusu olan bilişim sistemi, genellikle kurumların, işletmelerin veya gerçek kişilerin elektronik ortamda işlem yaptığı

platformları ifade eder (Kara, 2021: 225). Bu sistemlerde yer alan veriler ve programlar da doğrudan suçun konusu kapsamında değerlendirilir.

Suçun konusu olan bilişim sistemine yetkisiz erişim veya sistemde izinsiz kalma, sistemin işleyişini bozmanın yanı sıra, sistemde yer alan bilgilerin gizliliği, bütünlüğü ve erişilebilirliğine zarar verebilir. Bu nedenle, suçun konusu sadece fiziksel donanım değil, aynı zamanda bilişim sisteminin işlevselliği ve bilgi varlıklarıdır (İlhan, 2020: 138).

Sonuç olarak, TCK m. 243 kapsamında suçun konusu, bilişim sisteminin tamamı ve bu sistemde yer alan veriler olup, bu yapının korunması, suçun cezaî yaptırımlarının temel dayanağını oluşturmaktadır.

3.1.2.1.1.4. Hareket

Ceza hukukunda hareket, suçun maddi unsurunu oluşturan ve fail tarafından gerçekleştirilen fiilî davranışı ifade eder. Başka bir deyişle, hareket, failin iradesiyle dışa vurulan ve suçun gerçekleşmesini sağlayan fiilî davranıştır (Toroslu, 2020: 170). Suçun maddi unsurunun somutlaşabilmesi için hareketin varlığı zorunludur; hareket olmadan suçun gerçekleşmiş sayılması mümkün değildir.

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçu açısından hareket, failin gerçekleştirdiği dışa yönelik fiili ifade eder ve suçun maddi unsurunun temel bileşenlerinden biridir (Özgenç, 2019: 175). Hareket, bilişim sistemine yetkisiz erişim sağlama veya erişim hakkı sona erdikten sonra sistemde kalma şeklinde somutlaşır.

Maddenin uygulamasında failin gerçekleştirdiği hareket, bilişim sistemine giriş için şifrelerin kırılması, zararlı yazılım kullanımı veya doğrudan sistem arayüzüne izinsiz erişim gibi çeşitli şekillerde olabilir (Kara, 2021: 230). Ayrıca, failin sistemde izinsiz kalması, örneğin yetkisi sona eren bir hesabı kullanmaya devam etmesi ya da engelleme mekanizmalarını aşması şeklinde ortaya çıkar.

Hareketin suçun gerçekleşmesi için mutlaka bilerek ve isteyerek yapılması gerekir; yani failin kastı bulunmalıdır (İlhan, 2020: 142). Bu nedenle, failin hareketi kasten ve hukuka aykırı olarak gerçekleşmelidir.

Bilişim suçlarının doğası gereği, hareketler genellikle elektronik ortamda gerçekleştiğinden, delil toplama sürecinde bu hareketlerin tespiti ve kayıt altına alınması önem taşır (Özgenç, 2019: 177).

Sonuç olarak, TCK m. 243 kapsamındaki suçta hareket unsuru, bilişim sistemine yetkisiz erişim sağlama ve sistemde izinsiz kalma fiilleri ile şekillenmekte olup, failin hukuka aykırı ve kastlı eylemlerini kapsamaktadır.

3.1.2.1.1.5. Netice

Ceza hukukunda netice, failin gerçekleştirdiği hareketin dış dünyada yol açtığı somut sonucu ifade eder. Netice, özellikle sonuç sorumluluğu (neticeye bağlı suçlar) bakımından büyük öneme sahiptir; bazı suçlar, neticenin ortaya çıkmasıyla tamamlanmış sayılır. Neticenin varlığı, suçun maddi unsurunu tamamlayan temel unsurlardan biridir (Toroslu, 2020: 185).

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçu açısından netice, failin hareketi sonucunda ortaya çıkan ve suçun oluşması için gerekli olan hukuki sonucu ifade eder (Özgenç, 2019: 180). Bu suçun neticesi, bilişim sistemine yetkisiz olarak girilmesi veya yetkisi sona ermiş bir şekilde sistemde kalınmasıdır.

Netice, failin hukuka aykırı hareketi sonucu bilişim sisteminin işleyişinde veya güvenliğinde meydana gelen müdahaleyi kapsamaktadır. Bu müdahale, sistemin çalışmasının engellenmesi ya da sistem kaynaklarına yetkisiz erişimin sürdürülmesi şeklinde ortaya çıkabilir (Kara, 2021: 235). Ancak TCK m. 243 kapsamında suçun gerçekleşmesi için failin fiilinin doğrudan bir zarara yol açması şart değildir; yeterli olan bilişim sistemine izinsiz erişim ve sistemde kalmadır.

Suçun neticesi, bilişim sisteminin işleyişine veya veri güvenliğine ilişkin hukuki korunan değerin ihlal edilmesidir. Bu açıdan netice, failin hareketiyle bilişim sistemine hukuka aykırı müdahale gerçekleştirmesi sonucu doğar ve suçun oluşması için gerekli somut etkidir (İlhan, 2020: 145).

Sonuç olarak, TCK m. 243 kapsamındaki bilişim sistemine girme ve sistemde kalma suçunun neticesi, yetkisiz erişim veya sistemde kalma fiilinin gerçekleşmesi olup, failin kastı ile bu neticenin ortaya çıkması suçun maddi unsurlarını tamamlar.

3.1.2.1.2. Manevi Unsurlar

Ceza hukukunda manevi unsur, failin suç işleme iradesini ve bilincini ifade eden unsurdur. Başka bir deyişle, suçun oluşabilmesi için sadece fiilin dışa yansıması (maddi unsur) yeterli değildir; failin kast veya taksir gibi hukuken öngörülen manevi iradeye sahip olması gerekir (Toroslu, 2020: 200).

TCK m. 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçu bakımından manevi unsur, failin suçu işlerken taşıdığı psikolojik tutumu ifade eder ve genellikle kast olarak karşımıza çıkar (Özgenç, 2019: 183). Failin, bilişim sistemine yetkisiz bir şekilde girme veya yetkisi sona erdikten sonra sistemde kalma eylemini bilerek ve isteyerek gerçekleştirmesi gerekir.

Manevi unsurun gerçekleşebilmesi için failin, gerçekleştirdiği fiilin hukuka aykırı olduğunu bilmesi ve bu sonucu istemesi ya da sonucu öngörüp kabullenmesi gerekmektedir (Kara, 2021: 240). Buna göre, suça konu hareketin bilinçli ve iradi olması, suçun oluşması için zorunludur.

Bilişim suçlarının yapısı gereği, taksirle işlenmeleri mümkün değildir, dolayısıyla sadece kasıtlı davranışlar cezai sorumluluğa neden olur (İlhan, 2020: 149). Fail, sistemde kalma veya izinsiz giriş eyleminin hukuka aykırı olduğunu bilmek zorundadır. Ayrıca, failin suçu işlemek için gerekli ortamı bilerek ve isteyerek oluşturması da manevi unsurun bir parçasıdır.

Sonuç olarak, TCK m. 243 kapsamında suçu oluşturan manevi unsur, failin eylemini kastla gerçekleştirmesi olup, suçun oluşması için bilinçli ve isteyerek hareket etmesi zorunludur.

3.1.2.1.2.1. Kastın Unsurları

Failin kastı, sistemin kendisine ait olmadığını, bu sisteme girme hakkının bulunmadığını ve girişin hukuka aykırı olduğunu bilerek hareket etmesi anlamına gelir. Kast, doğrudan veya olası olabilir. Ancak uygulamada çoğunlukla doğrudan kast gündeme gelmektedir. Doğrudan kastta fail, bilişim sistemine izinsiz girmeyi ya da sistemde kalmayı bilerek ve isteyerek gerçekleştirir. Örneğin bir çalışanın, işverene ait sistemin şifresini değiştirerek ya da başka yollarla sisteme girmesi ve sistemde kalması, doğrudan kastla işlenmiş bir fiildir. (Kara, 2021: 250).

Buna karşılık, olası kast durumunda, fail eyleminin sonuçlarını öngörmekte ancak bu sonucun gerçekleşmesini kabullenmektedir. Ancak bilişim suçlarında bu türden kast uygulamaları oldukça sınırlıdır. Zira failin izinsiz erişimi sağlamak için genellikle aktif olarak bir dizi teknik ya da sosyal manipülasyon uygulaması gerekir. Bu da failin bilinçli ve istekli davrandığına işaret eder. (İlhan, 2020: 155).

3.1.2.1.2.2. Kastın Belirlenmesi

Uygulamada failin kastının varlığının tespiti, çoğu zaman teknik verilerle desteklenmektedir. Özellikle bilişim sistemlerine erişimde kullanılan araçlar (örneğin, parola kırıcı yazılımlar, IP yönlendirmeleri, VPN kullanımı, arka kapı yerleştirme vb.) failin eylemi planlı ve bilinçli gerçekleştirdiğine işaret eden somut deliller olarak değerlendirilir. (Kara, 2021: 260).

Doktrinde kastın değerlendirilmesinde şu unsurlar öne çıkar:

- Failin bilişim sistemine giriş yollarını bilmesi ve buna yönelik araçlar kullanması,
- Giriş eylemini gizlemeye çalışması (örneğin log dosyalarının silinmesi),
- Sistemden veri aktarmaya yönelik girişimlerde bulunması,
- Erişim sonrası sistemde belirli süre kalmaya devam etmesi.

Bu göstergeler failin eylemi bilinçli gerçekleştirdiğini desteklemektedir. (İlhan, 2020: 160).

3.1.2.1.2.3. Taksirin Mümkün Olmaması

Taksirli suç, dikkat ve özen yükümlülüğünün ihlaline dayanır. Ancak bilişim sistemine izinsiz girme gibi belirli bir teknik ve bilişsel eylem zinciri gerektiren bir suçta taksirle hareket edilmesi hukuken mümkün değildir. (Özgenç, 2019: 190). Örneğin, bir sistem yöneticisinin yanlışlıkla başka bir kişinin hesabına erişim sağlaması, eğer bu eylem izinsizliği bilmeden olmuşsa ve kötü niyet unsuru taşımıyorsa, suç oluşmaz; zira burada kastın varlığı aranır.

Taksirle sistemin zarar görmesi veya veri kaybına yol açılması halinde, farklı suç tipleri (örneğin görevi kötüye kullanma ya da kişisel verilerin ihlali) gündeme gelebilir, ancak TCK m. 243 anlamında suç oluşmaz (Kara, 2021: 270).

Bilişim sistemine izinsiz girme suçunda kast unsuru, failin eylemi bilerek ve isteyerek gerçekleştirmesi ile ortaya çıkar. Taksirle işlenmesi mümkün değildir. Failin kullandığı teknikler, eylemin planlı ve kasıtlı olduğunu ortaya koyar. Suçun manevi unsuru bakımından uygulamada genellikle doğrudan kast söz konusudur (İlhan, 2020: 165).

3.1.2.1.3. Hukuka Aykırılık

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçunda hukuka aykırılık, failin fiilinin hukuken korunmaya değer bir menfaate veya hukuki düzenlemeye karşı olmasıdır. Hukuka aykırılık, suçun maddi unsurunu tamamlayan temel unsurlardan biridir (Özgenç, 2019: 192).

Bilişim sistemine izinsiz giriş ve sistemde kalma fiilleri, failin yetkisiz olarak başkasının bilişim sistemine müdahale etmesi anlamına gelir. Bu müdahale, bilişim sistemine sahip kişinin veya kurumun meşru haklarını ihlal eder ve böylece fiilin hukuka aykırı olması söz konusu olur (Kara, 2021: 275).

Hukuka aykırılık unsuru, failin eyleminin herhangi bir hukuki sebep veya meşru müdafaa, yetki veya kanuni izin gibi nedenlerle haklı gösterilmemesi durumunda gerçekleşir (İlhan, 2020: 170). Örneğin, bilişim sistemine yetkili bir kişinin erişimi hukuka uygun iken, yetkisiz kişinin aynı erişimi hukuka aykırılık teşkil eder.

Bilişim suçlarında, hukuka aykırılık değerlendirilirken failin eyleminin etkilediği bilişim sisteminin sahibi veya kullanıcısının rızası ve yetkisi dikkate alınır. Rıza varsa hukuka aykırılık ortadan kalkar ve suç oluşmaz.

Sonuç olarak, TCK m. 243 kapsamındaki bilişim sistemine izinsiz girme suçunda hukuka aykırılık, failin yetkisiz şekilde sisteme müdahalesinin hukuki bir mazereti bulunmaması ile belirlenir ve suçun temel unsurlarından biridir.

3.1.2.1.3.1. Hukuka Aykırılık Kavramı

Hukuka aykırılık, ceza hukukunda bir fiilin suç sayılabilmesi için gerekli temel unsurlardan biridir. Genel anlamda, hukuka aykırılık, bir davranışın yürürlükteki hukuk normlarına ve hukuki düzenlemelere karşı olması durumunu ifade eder (Özgenç, 2019: 195). Başka bir ifadeyle, failin fiili hukuki bir hakka dayanmadığı ve hukuken geçerli bir mazeretinin bulunmadığı sürece, bu fiil hukuka aykırı sayılır.

Ceza hukukunda hukuka aykırılık, sadece kanunlara aykırı olmayı değil, aynı zamanda hukukun genel ilkelerine, adalet ve hakkaniyet prensiplerine de ters düşen davranışları kapsar. Hukuka aykırılık unsuru, suçun varlığını belirlemede fiilin normlara uygun olup olmadığının tespitini sağlar (Kara, 2021: 280).

Hukuka aykırılık, failin eyleminin herhangi bir hukuki savunma (örneğin, meşru müdafaa, kanuni yetki, zorunluluk hali) kapsamında olup olmaması ile ortadan kalkabilir. Eğer bu tür hukuki mazeretler varsa, fiil hukuka uygun hale gelir ve suç teşkil etmez (İlhan, 2020: 172).

Sonuç olarak, hukuka aykırılık, suçun oluşması için gerekli temel unsurlardan biri olup, failin eyleminin hukuk düzenine aykırı olduğunu ve geçerli bir hukuki sebebinin bulunmadığını ifade eder.

3.1.2.1.3.2. TCK M. 243 Açısından Hukuka Uygunluk Halleri

TCK m. 243 kapsamında düzenlenen fiilin hukuka uygun kabul edilebilmesi için bazı özel durumlar söz konusu olabilir. Bu bağlamda en sık karşılaşılan hukuka uygunluk nedenleri şunlardır:

3.1.2.1.3.2.1. Hakkın Kullanılması

TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme ve sistemde kalma suçunda, failin fiilinin hukuka aykırı olması suçun temel unsurlarından biridir. Ancak bazı durumlarda failin eylemi hukuka uygun sayılabilir ve bu durumlar hukuka uygunluk halleri olarak adlandırılır (Özgenç, 2019: 198).

Bunlardan biri hakkın kullanılmasıdır. Hakkın kullanılması, kişinin hukuken tanınmış bir hakkını meşru bir şekilde kullanmasıdır. Örneğin, bir sistem yöneticisi, görev yetkisi kapsamında bilişim sistemine erişim sağladığında, bu erişim hukuka uygundur ve TCK m. 243 kapsamındaki suç oluşmaz (Kara, 2021: 285).

Hakkın kullanılması savunması, failin eylemini hukuka uygun hale getirdiği için ceza sorumluluğunu ortadan kaldırır. Bu durumda, kişinin sistemde kalması veya sisteme giriş yapması yetkili ve yasal bir işlem olarak kabul edilir. Ayrıca, failin yetkisinin sona ermemiş olması veya yetkisinin yeniden verilmesi gibi durumlar da hukuka uygunluk halini oluşturur (İlhan, 2020: 175).

Sonuç olarak, TCK m.243 kapsamında, hakkın kullanılması hali, failin bilişim sistemine yetkili ve hukuka uygun olarak erişimini sağlar. Bu nedenle, failin yetkisi varsa veya yetkisi meşru bir şekilde verilmişse, eylem hukuka uygun sayılır ve suç oluşmaz.

3.1.2.1.3.2.2. Görevin İfa Edilmesi

TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme ve sistemde kalma suçunda, failin eyleminin hukuka aykırı olması gerekir. Ancak failin eylemi, görevini ifa etmesi kapsamında gerçekleşmişse, bu durum hukuka uygunluk hal**i** olarak değerlendirilir (Özgenç, 2019: 200).

Görevin ifası, kamu görevlisinin veya özel sektörde görevli personelin, kanuni veya iş sözleşmesine dayalı yetkilerini kullanarak bilişim sistemine erişim sağlaması anlamına gelir. Bu durumda fail, sistemde bulunmakla hukuka aykırı bir eylemde bulunmamış, aksine görevini yerine getirmiştir (Kara, 2021: 290).

Örneğin, bir kamu kurumunda çalışan sistem yöneticisinin, görev yetkisi dahilinde bilgi güvenliği veya bakım amacıyla bilişim sistemine girmesi hukuka uygundur. Aynı şekilde, işverenin talimatıyla çalışanların sistem erişim yetkilerinin kullanılması da görevin ifası kapsamında değerlendirilir (İlhan, 2020: 178).

Bu hukuka uygunluk hali, failin ceza sorumluluğunu ortadan kaldırır. Çünkü fail, hukuken kendisine tanınan bir yetkiyi kullanmaktadır ve eylemi suç teşkil etmez.

Sonuç olarak, TCK m. 243 kapsamındaki bilişim sistemine izinsiz girme suçunda, görevin ifası hukuka uygunluk sebebi olarak failin sorumluluğunu kaldırır.

3.1.2.1.3.2.3. İlgilinin Rızası

TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme suçunda failin fiilinin hukuka aykırı olması gerekir. Ancak, failin eylemine konu bilişim sisteminin sahibi veya yetkili kullanıcısının rızası bulunması durumunda, hukuka aykırılık ortadan kalkar ve suç oluşmaz (Özgenç, 2019: 202).

İlgilinin rızası, sistem sahibinin veya yetkili kişinin, failin bilişim sistemine girişine ve sistemde kalmasına onay vermesi anlamına gelir. Bu rıza açık ya da zımni olabilir. Açık rıza, doğrudan ve bilinir şekilde verilen izin iken, zımni rıza, örneğin işveren tarafından çalışanlarına sistem erişim izni verilmesi gibi dolaylı yollarla gerçekleşir (Kara, 2021: 295).

Rızanın varlığı, failin eyleminin hukuki bir dayanağa sahip olduğunu gösterir ve bu nedenle suçun hukuka aykırılık unsurunu ortadan kaldırır (İlhan, 2020: 180). Ancak rızanın, hukuka aykırı amaçlarla verilmemiş ve geçerli olması gerekir; aksi takdirde hukuka uygunluk doğmaz.

Sonuç olarak, TCK m. 243 kapsamında bilişim sistemine izinsiz girme suçunda, ilgilinin geçerli rızası hukuka uygunluk sebebi olup, failin eyleminden dolayı ceza sorumluluğu doğmaz.

3.1.2.1.3.2.4. Hukuka Uygunluk Halleri Olmaksızın Erişim

Eğer yukarıda sayılan hukuka uygunluk nedenlerinden hiçbiri mevcut değilse, sistem sahibinin açık izni olmaksızın sisteme girilmesi veya sistemde kalınması fiili hukuka aykırı kabul edilir. Bu durumda suçun maddi ve manevi unsurları tamamlanmış olur ve fail cezai sorumluluk taşır (Özgenç, 2019: 210).

Özellikle özel hayatın gizliliği, haberleşmenin mahremiyeti gibi anayasal güvence altındaki değerlerin ihlal edildiği durumlarda, sistem erişiminin hukuka aykırılığı daha da ağırlaşmaktadır. Bu nedenle bilişim suçlarıyla mücadelede hukuka uygunluk değerlendirmesi yalnızca teknik değil, aynı zamanda anayasal perspektifle de ele alınmalıdır (Kara, 2021: 310).

Bilişim sistemine girme ve sistemde kalma fiilinin hukuka aykırı sayılabilmesi için, eylemin hukuka uygunluk nedenleriyle örtüşmemesi gerekir. Bu suç tipi bakımından özellikle ilgilinin rızası, görev gereği erişim ve hakkın kullanılması gibi nedenler hukuka aykırılığı ortadan kaldırabilir. Aksi durumda, tipiklik taşıyan her fiil, hukuka aykırılık unsurunu da taşır ve cezai sorumluluğa yol açar (İlhan, 2020: 185).

3.1.2.1.4. Suçun Özel Görünüş Biçimleri

Ceza hukuku teorisinde, suçların yalnızca tamamlanmış halleri değil, tamamlanmadan önceki safhaları ve birden fazla kişiyle birlikte işlenme durumları da hukuki değerlendirmeye tabi tutulur. Bu kapsamda suçun özel görünüş biçimleri; teşebbüs, iştirak ve içtima olarak üç ana başlıkta ele alınır (Aksu, 2018: 120).

TCK m. 243 kapsamında düzenlenen bilişim sistemine izinsiz erişim suçu bakımından da bu unsurlar büyük önem taşımaktadır. Suçun oluşum sürecinde, failin eylemini tamamlamadan önce müdahalesi teşebbüs kapsamında değerlendirilirken,

birden fazla failin birlikte hareket etmesi iştirak kavramı ile açıklanır. Ayrıca, aynı eylemle birden fazla suçun oluşması halinde içtima hükümleri gündeme gelir (Özgenç, 2019: 215).

Bu bağlamda, bilişim sistemine izinsiz girme suçunda failin eyleminin teşebbüs aşamasında kalması halinde, cezai sorumluluk doğar; ancak suçun tamamlanmamış olması indirim sebebi olabilir. İştirak halinde ise, fiile katılan her kişinin sorumluluğu, katkı derecesine göre değerlendirilir (Kara, 2021: 315).

TCK m. 243 kapsamında suçun özel görünüş biçimleri, suçun oluşumunun bütüncül şekilde anlaşılması ve failin sorumluluğunun doğru tespit edilmesi açısından önemlidir.

3.1.2.1.4.1. Teşebbüs

Ceza hukukunda teşebbü**s**, suçun tamamlanması için gerekli olan eylemin kısmen gerçekleştirilmesi ancak çeşitli sebeplerle tamamlanamaması durumudur (Aksu, 2018: 130). TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme suçu bakımından teşebbüs, failin bilişim sistemine izinsiz giriş veya sistemde kalma eylemini tamamlamadan önce müdahalesi anlamına gelir (Özgenç, 2019: 220).

Bilişim suçları özelinde teşebbüsün değerlendirilmesinde failin eyleminin teknik olarak engellenmesi veya bilinçli olarak yarıda bırakılması önemlidir. Örneğin, bir kişinin sisteme girmek için şifre kırma denemesi yapması, ancak sistem tarafından engellenmesi teşebbüs halini oluşturur (Kara, 2021: 320).

Örneğin, failin şifre kırıcı bir yazılım aracılığıyla sisteme sızmaya çalışması ancak yazılımın durdurulması veya IP adresinin engellenmesi sonucu sisteme erişememesi, açıkça teşebbüs olarak değerlendirilir.

TCK m. 243 kapsamında teşebbüs, tamamlanmamış suç olarak kabul edilmekle birlikte, failin ceza sorumluluğunu ortadan kaldırmaz. Kanun, teşebbüs hallerinde genellikle cezada indirim imkanı tanır; çünkü fail eylemini tamamlamamış olsa da hukuka aykırı girişimde bulunmuştur (İlhan, 2020: 190).

Hukuki sonuç olarak, teşebbüs hâlinde cezada indirim yapılabileceği gibi, eylemin ağırlığına göre indirim yapılmayabilir (TCK m. 35/2).

3.1.2.1.4.2. İştirak

Ceza hukuku kapsamında iştirak, bir suçu birden fazla kişinin birlikte ve ortak iradeyle işlemesi durumudur. İştirak, fail ile yardım eden veya azmettiren kişilerin hukuki sorumluluklarının belirlenmesinde önemli bir kavramdır (Aksu, 2018: 140).

TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme suçunda da iştirak kavramı uygulanmaktadır. Suçun işlenmesinde birden fazla kişinin rol alması halinde, failin yanı sıra suçu kolaylaştıran, yardım eden veya azmettiren kişiler de ceza sorumluluğu taşır (Özgenç, 2019: 225).

İştirak şekilleri genel olarak üçe ayrılır: birlikte hareket eden fail (müteselsil fail), yardım eden ve azmettiren. Örneğin, bir kişinin bilişim sistemine izinsiz erişim sağlaması, diğerinin teknik destek veya şifre temini gibi yardımda bulunması iştirak kapsamına girer (Kara, 2021: 325).

Müşterek faillik durumunda, örneğin bir kişinin sistem açığını tespit edip diğer kişinin sisteme girmesi durumunda, her iki kişi de suça iştirak etmiş sayılır.

Azmettirme, failin sistemi hedef almasına başkasının yönlendirmesiyle karar vermesiyle oluşur. Örneğin, bir işvereni cezalandırmak amacıyla bir başkasına sistemine girme talimatı vermek, azmettirme olarak değerlendirilir.

Yardım etme, doğrudan fiili işlemeyen ancak araç temin eden, bilgi sağlayan veya sistemin açığını hazırlayan kişiler için söz konusudur. Bu kişilerin cezası, asli faile göre daha hafif belirlenir

TCK m. 243 bağlamında, iştirak eden herkes işlenen suça ortak sayılır ve sorumlulukları failin sorumluluğu ile paralel olarak değerlendirilir. Ancak iştirak derecesi ve katkı biçimi cezada belirleyici olabilir (İlhan, 2020: 195).

Uygulamada, bilişim suçları genellikle teknik bilgi ve uzmanlık gerektirdiğinden, suçun iştirak hâlinde işlenmesi oldukça yaygındır. Bu nedenle, iş bölümü yapılarak suçun gerçekleştirilmesi hâlinde her bir failin rolü detaylı olarak değerlendirilmeli ve kastın yoğunluğu dikkate alınmalıdır.

3.1.2.1.4.3. İçtima

Ceza hukuku açısından içtima, aynı fiille birden fazla suçun işlenmesi durumunda ortaya çıkan sorumluluk ve ceza uygulamalarını ifade eder. İçtima, failin işlediği suçlar arasında ceza adaletinin sağlanması amacıyla uygulanan kurallar bütünüdür (Aksu, 2018: 150).

İçtima, birden fazla suçun tek bir fiille veya birkaç fiille işlenmesi durumunda, faile hangi suçlardan dolayı ve kaç ceza verileceğinin belirlenmesini konu alır. TCK' nın 42–44. maddelerinde düzenlenen içtima kuralları, özellikle bilişim sistemine izinsiz girme suçunun başka suçlarla birlikte işlenmesi hâlinde devreye girmektedir (Aksu, 2018: 150; Özgenç, 2019: 230).

TCK'nın 243. maddesinde düzenlenen bilişim sistemine izinsiz girme suçunda da içtima hükümleri önem taşır. Örneğin, fail aynı bilişim sistemine izinsiz giriş yaparken, farklı zamanlarda veya farklı yöntemlerle birden fazla suç oluşturabilir. Bu durumlarda, içtima kuralları gereğince cezaların nasıl belirleneceği değerlendirilir (Özgenç, 2019: 230).

İçtima iki ana türde gerçekleşebilir: gerçek içtima ve şahsi içtima. Gerçek içtima, aynı fiilin birden çok suç oluşturması durumunda ortaya çıkar. Örneğin, bir bilişim sistemine izinsiz girme eylemi aynı zamanda kişisel verilerin hukuka aykırı olarak ele geçirilmesini de içeriyorsa, bu durum gerçek içtimaya örnek teşkil eder (Özgenç, 2019: 231).

Şahsi içtima ise failin farklı zamanlarda veya farklı eylemlerle birden çok suç işlemesi hâlidir. TCK m. 243 kapsamında, bir fail farklı zamanlarda aynı sisteme izinsiz giriş yaparsa veya sistemde kalma ve veri aktarımı gibi ayrı fiiller gerçekleştirirse, şahsi içtima durumu söz konusu olur (Kara, 2021: 335).

Bilişim sistemine izinsiz giriş suçu açısından, suçun tamamlanmadan önceki aşamaları (teşebbüs), çok faille işlenmesi (iştirak) ve başka suçlarla bağlantısı (içtima) hukuki açıdan oldukça önemlidir. Özellikle teşebbüs durumunda ceza indirimi, iştirak hâlinde her failin rolüne göre ceza tayini ve içtima durumunda suçların birbirinden ayrıştırılması, ceza adaletinin sağlanması açısından temel unsurlardır. Bilişim suçlarının teknik boyutları nedeniyle bu özel görünüş biçimlerinin dikkatli incelenmesi gerekmektedir.

3.1.2.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (M. 244/1-2)

3.1.2.2.1. Maddi Unsurlar

Ceza hukukunda bir suçun oluşabilmesi için belirli unsurların varlığı gereklidir. Bu unsurlardan biri olan maddi unsur, suç tipinde yasaklanan fiilin dışa yansıyan ve gözlemlenebilir biçimde gerçekleşmiş olmasını ifade eder. Başka bir deyişle, maddi unsur, suçun fiilî yönü olarak tanımlanabilir ve suçun objektif görünüşünü oluşturur (Toroslu, 2020: 112). Maddi unsur, yalnızca suç fiilinin gerçekleşmiş olmasını değil, aynı zamanda bu fiilin kanunda öngörülen şekil ve niteliklere uygunluğunu da kapsar.

Maddi unsur, ceza hukukunda diğer unsurlardan, özellikle manevi unsurdan ayrılır. Manevi unsur, failin suç işleme iradesini ve kastını ifade ederken, maddi unsur yalnızca eylemin dışa yansıyan biçimsel varlığını kapsar. Bu ayrım, suçun hem objektif hem de subjektif yönlerinin doğru bir şekilde değerlendirilmesi açısından büyük önem taşır (Aksoy, 2018: 76).

TCK'nın 244. maddesi, bilişim sistemlerine yönelik saldırılar kapsamında, sistemin işleyişini engelleme, bozma, verileri yok etme veya değiştirme eylemlerini düzenlemektedir. Bu suçun maddi unsurları, failin bilişim sistemine yönelik müdahalede bulunması ile gerçekleşir. Burada kritik olan, fiilin bilişim sisteminin işleyişini engellemesi veya bozmasıdır. Ayrıca sistemde bulunan verilerin kısmen veya tamamen yok edilmesi ya da değiştirilmesi de bu kapsamda değerlendirilir (Özgenç, 2019: 245). Failin eylemi, sistemin normal işleyişine zarar verecek ya da verilerin bütünlüğünü ortadan kaldıracak nitelikte olmalıdır.

3.1.2.2.1.1. Fail

Ceza hukukunda fail, suç tipinde yasaklanan fiili gerçekleştiren aktif süje olarak tanımlanır. Fail, yalnızca fiili gerçekleştiren kişi değil, aynı zamanda bu fiilin hukuka aykırı olduğunu bilerek ve isteyerek hareket eden kişidir. Bu bağlamda failin eylemi, suçun maddi unsuru ile doğrudan bağlantılıdır; yani suçun dışa yansıyan fiilî yönünü fail gerçekleştirmektedir (Toroslu, 2020: 98).

TCK'nın 244. maddesinde düzenlenen "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme" suçunun failinin belirlenmesi, suçun temel unsurlarından biridir.

Bu suçun faili, bilişim sistemine yönelik müdahaleyi gerçekleştiren gerçek kişi ya da kişiler olabilir.

Failin, bilişim sistemine erişim hakkı olan veya olmayan olması durumu suçun oluşumunu değiştirmez. Yetkisi olmaksızın sisteme giren kişi, doğrudan suçun faili olur. Ancak bazen sistem yöneticisi, çalışan ya da yetkili kişiler, erişim yetkilerini kötüye kullanarak bilişim sistemini bozabilir, engelleyebilir veya verileri yok edebilir. Bu durumlarda da fail, sistem üzerindeki yetkisini kötüye kullanan kişi olarak sorumludur (Kara, 2021: 351).

Ayrıca, suçun işlenmesinde kastın varlığı önemli olup, failin bilinçli ve isteyerek bu eylemleri gerçekleştirmesi gerekir. Failin amacı, bilişim sisteminin işleyişini engellemek, bozmak veya verilerin bütünlüğünü ortadan kaldırmaktır (Aksu, 2018: 176).

TCK m. 244/1-2 suçu bakımından fail, sistemi engelleme, bozma veya verileri yok etme/değiştirme eylemini gerçekleştiren gerçek kişi olup, ister sisteme yetkisiz erişim sağlamış ister yetkisini kötüye kullanmış olsun, cezai sorumluluk yüklenir (Özgenç, 2019: 246).

Bilgisayar ve bilişim teknolojilerinde uzmanlaşan kişiler, bu tür suçların failleri arasında daha sık rastlanan gruplar arasındadır.

3.1.2.2.1.2. Mağdur

Ceza hukukunda mağdur, suçtan doğrudan zarar gören gerçek veya tüzel kişiyi ifade eder. Mağdur, suçun işlendiği eylemden etkilenen ve hukuken korunması gereken kişidir. Mağdurun varlığı, suçun toplumsal ve bireysel etkilerini anlamak açısından önemlidir. Ceza hukuku, mağdurun haklarını korumayı, zararının giderilmesini ve adaletin sağlanmasını temel amaçlar arasında görür (Toroslu, 2020: 145).

TCK m. 244/1-2'de düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunda mağdur, doğrudan zarar gören kişi veya kurumu ifade eder. Bu mağdur, suçun işlendiği bilişim sisteminin sahibi, işletmecisi veya hukuken korunan menfaatine sahip gerçek ya da tüzel kişiler olabilir (Kara, 2021: 353).

Mağdurun temel zararları, sistemin çalışamaz hale gelmesi, verilerin kaybı, verilerin değiştirilmesi nedeniyle uğranan maddi ve manevi zararlar şeklinde ortaya çıkar.

Özellikle kamuya açık bilişim sistemlerine yönelik eylemlerde, mağdur toplumun genelidir ve zarar toplumsal boyut kazanır (İlhan, 2020: 225).

Bilişim sistemlerinin güvenliği ve bütünlüğü, mağdurun kişisel, kurumsal ve toplumsal çıkarlarını koruyan anayasal ve yasal düzenlemelerle güvence altına alınmıştır. Bu nedenle mağdurun korunması, suçun cezalandırılmasının temel amaçlarından biridir (Özgenç, 2019: 249).

TCK m. 244/1-2 suçunda mağdur, sistemi kullanan ve eylem nedeniyle doğrudan zarar gören kişi veya kurumdur. Bu zarar, sistemin işleyişinin aksaması, verilerin tahribi veya yok edilmesi yoluyla gerçekleşir.

Örneğin, bir bankanın ödeme sistemine yapılan müdahale sonucu müşterilerin işlemleri etkilenebilir. Mağdurun hukuki menfaati, bu suçta özellikle korunmaya değerdir çünkü bilişim sistemleri çağımızda bilgi ve iletişim altyapısının temelini oluşturur.

3.1.2.2.1.3. Suçun Konusu

Ceza hukukunda suçun konusu, failin işlediği suç fiilinden zarar gören veya fiilin yöneldiği nesne ya da değerleri ifade eder. Başka bir deyişle, suçun konusu, hukuka aykırı eylemin etkilediği hukuki değer veya menfaatlerdir. Suçun konusu, failin eyleminden etkilenen bireyler, toplum veya kamu düzeni olabileceği gibi, malvarlığı, kişilik hakları, kamu güvenliği gibi soyut değerler de olabilir (Toroslu, 2020: 159).

TCK m. 244/1-2'de düzenlenen suçun konusu, bilişim sistemleri ve bu sistemlerde yer alan veriler ile bilişim sistemlerinin işleyişini sağlayan donanım ve yazılım bütünüdür. Suçun maddi nesnesi, bu unsurların hukuka aykırı şekilde engellenmesi, bozulması, yok edilmesi veya değiştirilmesi suretiyle zarar görmesidir (Özgenç, 2019: 245).

Bilişim sistemi, elektronik ortamda verilerin depolandığı, işlendiği ve yönetildiği bütünleşik bir yapıdır. Bu yapıyı oluşturan donanım (sunucular, bilgisayarlar, ağ cihazları vb.) ve yazılım (işletim sistemleri, uygulamalar, veri tabanları vb.) unsurları, suçun korunma alanını oluşturur (Kara, 2021: 349).

Ayrıca, suçun konusu kapsamında yer alan veriler, sistemde depolanan her türlü bilgi, belge, kayıt ve elektronik dokümanı içerir. Bu veriler üzerinde yapılan yok etme

veya değiştirme eylemleri, sistemin işleyişini ve veri bütünlüğünü doğrudan etkiler (İlhan, 2020: 222).

TCK m. 244/1-2 suçu, bilişim sistemlerinin işleyişini sağlayan teknik altyapı ile bu altyapı üzerinde bulunan verilerin tamamını kapsar ve bunların hukuka aykırı şekilde zarar görmesi suçun konusunu oluşturur.

3.1.2.2.1.4. Hareket

Ceza hukukunda hareket, suçun maddi unsurunu oluşturan ve fail tarafından gerçekleştirilen fiilî davranışı ifade eder. Başka bir deyişle, hareket, failin iradesiyle dışa vurulan ve suçun gerçekleşmesini sağlayan fiilî davranıştır (Toroslu, 2020: 170). Suçun maddi unsurunun somutlaşabilmesi için hareketin varlığı zorunludur; hareket olmadan suçun gerçekleşmiş sayılması mümkün değildir.

TCK m. 244/1-2'de düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunda hareket unsuru, failin bilişim sistemine yönelik hukuka aykırı eylemlerini ifade eder. Bu hareketler, bilişim sisteminin işleyişine zarar veren veya veri bütünlüğünü ortadan kaldıran fiilleri kapsar (Özgenç, 2019: 246).

Hareket, suçun maddi unsurunu oluşturur ve kanunda açıkça belirtilen davranışları kapsar. TCK m. 244/1 ve m. 244/2'de düzenlenen hareketler farklılık gösterir:

3.1.2.2.1.4.1. TCK m. 244/1 De Düzenlenen Hareketler

Birinci fıkrada yer alan hareketler; bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna konu olan hareketler açıkça tanımlanmıştır. Bu hareketler, bilişim sistemlerinin güvenliğini ve işleyişini doğrudan etkileyen hukuka aykırı fiiller olarak karşımıza çıkar (Özgenç, 2019: 245). Örneğin, bir sisteme zarar verici yazılım yerleştirmek, sistemin veri akışını kesintiye uğratmak, sistemdeki verileri silmek veya değiştirmek gibi hareketler bu kapsamda değerlendirilir.

Bu eylemler, sistemin işleyişine doğrudan müdahaleyi içerir ve sistemin fonksiyonel kapasitesini azaltır veya tamamen ortadan kaldırır. Ayrıca, bu tür hareketler sistemdeki verilerin güvenilirliğini ve bütünlüğünü de tehdit eder. Bilgi güvenliği açısından, sistemin bu tür saldırılardan korunması ulusal ve uluslararası hukukta önemli bir yer tutar.

3.1.2.2.1.4.2. TCK m. 244/2 De Düzenlenen Hareketler

İkinci fıkrada ise, birinci fıkrada düzenlenen suçun sonucu olarak ortaya çıkan hallerin cezalandırılması amaçlanmıştır. Bu fıkrada belirtilen hareketler, suçun zarar verici etkisinin daha ciddi olduğu durumları kapsar. TCK m. 244/2 kapsamında fail, bilişim sisteminin işleyişini engelleme veya bozma fiillerini, sistemin devamlılığı veya kamu hizmetlerinin ifası açısından kritik öneme sahip olması durumunda gerçekleştirir. Örneğin, devlet kurumlarına ait kritik bilişim altyapılarına yönelik saldırılar veya sağlık, enerji, ulaşım gibi kamu hizmetlerini doğrudan etkileyen sistemlere zarar verme halleri bu kapsamda yer alır (Kara, 2021: 355).

Ayrıca, verilerin yok edilmesi veya değiştirilmesi fiilleri, sistemin işleyişinde telafisi güç zararlar meydana getiriyorsa TCK m. 244/2 kapsamında değerlendirilir. Bu fiiller, genellikle zararlı yazılım kullanımı, sistematik veri manipülasyonu veya yaygın veri silme gibi yöntemlerle yapılır ve failin eyleminin sonuçları ağırdır (İlhan, 2020: 230).

TCK m. 244/2 maddesinde düzenlenen hareketler, daha kapsamlı ve sistematik zarar verme niyetini içerir. Bu nedenle failin eylemleri genellikle planlı, hedefli ve etkileri itibarıyla geniş çaplıdır. Suçun bu derecesi, cezada artırımı gerektiren nitelikli haller olarak kabul edilir (Özgenç, 2019: 252).

TCK m. 244/2'de yer alan hareketler, bilişim sistemlerinin kritik unsurlarına yönelik ağır zarar verme eylemlerini ifade eder ve failin bu hareketleri bilinçli, sistematik ve ağır sonuçlar doğuracak şekilde gerçekleştirmesi gerekir.

3.1.2.2.2. Manevi Unsurlar

Ceza hukukunda manevi unsur, failin suç işleme iradesini ve bilincini ifade eden unsurdur. Başka bir deyişle, suçun oluşabilmesi için sadece fiilin dışa yansıması (maddi unsur) yeterli değildir; failin kast veya taksir gibi hukuken öngörülen manevi iradeye sahip olması gerekir (Toroslu, 2020: 200).

TCK m. 244/2'de düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun manevi unsuru, failin eylemini bilerek ve isteyerek gerçekleştirmesidir. Manevi unsur, yani kast, suçun oluşumu için zorunludur ve failin suçun hukuki ve fiili unsurlarını bilmesi ile istekli olması anlamına gelir (Özgenç, 2019: 248).

Bu kapsamda fail, bilişim sistemine zarar verme amacını taşımalı ya da zarar verme sonucunu bilerek ve istemeyerek kabullenmelidir. Özellikle TCK m. 244/2'deki hareketlerin ağırlığı ve sonuçları göz önüne alındığında, genellikle doğrudan kastla hareket edildiği kabul edilir. Failin, bilişim sistemine verdiği zararın etkilerini öngörmemesi veya istememesi durumunda bile, eylemi sonucu doğuracak hareketlerde bilinçli taksir tartışılmaz (Kara, 2021: 360).

Manevi unsurun değerlendirilmesinde, failin eylemi planlama şekli, kullandığı teknik araçlar, hedef aldığı sistemin önemi ve zarar verme kastı önemli göstergeler olarak ortaya çıkar. Örneğin, kritik kamu altyapılarına yönelik kasıtlı saldırılar, failin doğrudan kastla hareket ettiğinin açık göstergesidir (İlhan, 2020: 235).

TCK m. 244/2 kapsamında suçun manevi unsuru, failin bilişim sistemine zarar verme iradesi ve bilinciyle hareket etmesidir. Kast, hem doğrudan hem de olası kast şeklinde ortaya çıkabilir; ancak ağır ve sistematik zarar verme suçlarında çoğunlukla doğrudan kast hâkimdir.

3.1.2.2.3. Hukuka Aykırılık

Ceza hukuku açısından hukuka aykırılık, failin işlediği fiilin toplum düzenine ve hukuki kurallara aykırı olmasıdır. TCK m. 244/2'de düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunda da hukuka aykırılık unsuru, failin bilişim sistemine yönelik hareketlerinin herhangi bir hukuka uygunluk nedenine dayanmayarak gerçekleştirilmesidir (Özgenç, 2019: 253).

Bu bağlamda, failin eylemi; meşru müdafaa, yetkili makamın emri, kanuni izin veya ilgilinin açık rızası gibi hukuka uygunluk halleri bulunmadıkça hukuka aykırı kabul edilir. Özellikle TCK m. 244/2'deki hareketler, kamu hizmetlerine veya kritik altyapılara yönelik olduğunda, bu hukuka aykırılık daha da ağırlaşır ve toplumsal zararları artırır (Kara, 2021: 365).

Hukuka uygunluk halleri olmaksızın gerçekleştirilen bilişim sistemine zarar verme eylemleri, suçun tipiklik ve hukuka aykırılık unsurlarını tamamlar. Failin davranışının hukuki koruma altındaki değerlerle çelişmesi durumunda, ceza sorumluluğu doğar (İlhan, 2020: 238).

TCK m. 244/2 suçunda hukuka aykırılık, failin bilişim sistemine zarar verme fiilini hukuka uygunluk nedenleri olmadan gerçekleştirmesiyle oluşur ve suçun temel unsurudur.

3.1.2.2.4. Suçun Özel Görünüş Biçimleri

3.1.2.2.4.1. Teşebbüs

TCK m. 244/2 maddesinde düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarında teşebbüs hali mümkündür. Teşebbüs, failin suçun tamamlanması için gerekli olan eylemi bilinçli olarak başlatması ve suçun tamamlanmasına yönelik niyetinin bulunmasıdır; ancak, çeşitli nedenlerle suç tamamlanmamışsa teşebbüsten söz edilir (Özgenç, 2019: 256).

Bilişim suçlarında teşebbüsün tespiti genellikle teknik delillerle desteklenir. Örneğin, sisteme zarar verme amacıyla zararlı yazılım yüklemek için girişimde bulunan ancak sistemin güvenlik önlemleri nedeniyle fiilin tamamlanamaması teşebbüs olarak değerlendirilir. Fail, suçun tamamlanması için gerekli hareketleri yapmış ancak dışsal engeller nedeniyle zarar gerçekleşmemiştir (Kara, 2021: 370).

Teşebbüs halinde, failin kastı ve suç işleme iradesi tamdır, ancak sonuç gerçekleşmemiştir. Bu durum, bilişim suçlarında suçun ağır zarar verme boyutlarına göre farklı ceza uygulamalarına sebep olabilir. Ceza hukukunda teşebbüs, suçun tamamlanmasına göre daha hafif cezalandırılır ancak failin kusuru ve niyeti göz önünde bulundurulur (İlhan, 2020: 240).

TCK m. 244/2'de yer alan bilişim suçlarında teşebbüs, failin suç işleme kararını uygulamaya koyması ancak eylemin tamamlanamaması durumudur ve ceza sorumluluğunu doğurur.

3.1.2.2.4.2. İştirak

TCK m. 244/2 düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunda iştirak hali, suçun birden fazla kişi tarafından birlikte işlenmesi durumunu ifade eder. İştirak; fail, yardım eden ve azmettiren gibi farklı rollerle ortaya çıkabilir ve her bir kişinin cezai sorumluluğu, katkı derecesine göre belirlenir (Özgenç, 2019: 260).

Bilişim suçlarında iştirak, teknik bilgi ve imkânların paylaşılması, zararlı yazılım geliştirilmesi, sisteme izinsiz erişimde birlikte hareket edilmesi veya eylemin farklı safhalarında destek sağlanması şeklinde ortaya çıkabilir. Örneğin, bir kişi zararlı yazılımı geliştirirken, diğeri bu yazılımı kullanarak sistemi hedef alabilir. Bu durumda her iki kişi de suçun faili olarak değerlendirilir (Kara, 2021: 375).

İştirak halinin tespiti ve cezai yaptırımı bakımından, failin eyleme katkısı, suça bilerek katılımı ve kastının bulunması önemlidir. İştirak halinde, tüm katılımcılar işledikleri suçun sorumluluğunu taşır; ancak, ceza tayininde katkı dereceleri dikkate alınabilir (İlhan, 2020: 245).

TCK m. 244/2 kapsamındaki bilişim suçlarında iştirak, suçun birden fazla kişi tarafından birlikte işlenmesini ifade eder ve her bir katılımcının sorumluluğu ayrı ayrı değerlendirilir.

3.1.2.2.4.3. İçtima

Ceza hukukunda içtima, birden fazla suçun tek bir fiille veya birkaç fiille işlenmesi durumunda faile verilecek cezanın belirlenmesini düzenleyen hukuki kavramdır. TCK'nın 42 ila 44. maddeleri, içtima kurallarını kapsamlı şekilde ele almaktadır (Özgenç, 2019: 265).

Bilişim suçları bağlamında, özellikle TCK m. 244/2'de düzenlenen sistemin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçları, genellikle başka suçlarla birlikte işlenebilmektedir. Örneğin, aynı olayda bilişim sistemine izinsiz girme (TCK m. 243), kişisel verilerin hukuka aykırı olarak ele geçirilmesi (KVKK kapsamında), ya da haberleşmenin engellenmesi gibi diğer suçlar da söz konusu olabilir. Bu durumda içtima hükümleri devreye girer.

İçtima, iki şekilde ortaya çıkar:

- Gerçek İçtima: Failin farklı zamanlarda birden fazla suçu işlemesi durumudur. Örneğin, bilişim sistemine izinsiz girme ve ardından sistemde veri değişikliği yapma suçlarını ayrı ayrı işlemesi.
- Hukuki İçtima: Tek fiil ile birden fazla suçun işlenmesidir. Örneğin, sistemde yapılan bir eylemin hem sistemi engelleme hem de verileri değiştirme suçlarını oluşturması.

TCK m. 42-44 hükümleri, içtimaya konu suçlarda hangi cezanın nasıl verileceğini belirler. Genel olarak, fail hakkında verilen cezalar, daha ağır olan cezanın artırılması veya ceza birleştirilmesi yoluyla uygulanır (Kara, 2021: 380).

Bilişim suçlarında içtima değerlendirilirken, suçların birbirinden ayrılması, suçun niteliği, failin kastı ve suçların işlenme şekli önem kazanır. Örneğin, TCK m. 244/2 kapsamında gerçekleşen zarar verme hareketi, TCK m. 243'teki izinsiz erişim suçu ile birlikte işlendiğinde, ceza tayininde içtima kuralları uygulanır (İlhan, 2020: 250).

TCK m. 244/2 suçunda içtima, failin işlediği birden fazla suçun ceza hukuku açısından nasıl değerlendirileceğini belirler ve ceza miktarının adil bir şekilde tayin edilmesi için önemli bir hukuki mekanizmadır.

3.1.2.3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (TCK m. 244/4)

Bilişim teknolojilerinin gelişimi, ekonomik ve sosyal yaşamın birçok alanında yeni fırsatlar sunarken, suç işleme yöntemlerinde de önemli değişikliklere yol açmıştır. Bu gelişmeler karşısında ceza hukuku, bilişim sistemleri aracılığıyla işlenen suçları tanımlamak ve yaptırımlarını belirlemek zorunda kalmıştır. TCK'nın 244. maddesinin 4. fıkrası, bilişim sistemleri kullanılarak hukuka aykırı yarar sağlanmasını düzenlemekte ve bu suça ilişkin ceza hükümlerini içermektedir.

Bu maddede amaç, bilişim sistemleri üzerinden elde edilen haksız menfaatlerin önüne geçmek, ekonomik düzenin korunmasını sağlamak ve bilişim suçlarının etkili bir şekilde cezalandırılmasını temin etmektir.

3.1.2.3.1. Maddi Unsurlar

Ceza hukukunda bir suçun oluşabilmesi için belirli unsurların varlığı gereklidir. Bu unsurlardan biri olan maddi unsur, suç tipinde yasaklanan fiilin dışa yansıyan ve gözlemlenebilir biçimde gerçekleşmiş olmasını ifade eder. Başka bir deyişle, maddi unsur, suçun fiilî yönü olarak tanımlanabilir ve suçun objektif görünüşünü oluşturur (Toroslu, 2020: 112). Maddi unsur, yalnızca suç fiilinin gerçekleşmiş olmasını değil, aynı zamanda bu fiilin kanunda öngörülen şekil ve niteliklere uygunluğunu da kapsar.

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu, maddi unsur bakımından failin bilişim sistemini kullanarak haksız maddi menfaat elde etme eylemi ile

gerçekleşir. Bu suçun maddi unsuru, failin bilişim sistemi üzerinden doğrudan veya dolaylı olarak bir kazanç sağlamasıdır (Özgenç, 2019: 278).

Maddi unsurun oluşabilmesi için failin, bilişim sisteminde yer alan verileri veya sistemi kullanarak; para, mal, hizmet veya diğer ekonomik değerler şeklinde hukuka aykırı bir çıkar elde etmesi gerekir. Örneğin, bir banka çalışanının yetkisi olmadan müşteri hesaplarını manipüle ederek haksız kazanç sağlaması veya siber suçluların sahte işlemlerle maddi çıkar elde etmesi durumları bu kapsamda değerlendirilebilir (Kara, 2021: 405).

Bilişim sistemi aracılığıyla sağlanan yarar, sadece failin kendisine değil, başkalarına da sağlanabilir. Bu noktada suçun faili, yararı elde eden kişi olabileceği gibi, yararı başkaları için temin eden kişi de olabilir. Failin eylemi, sistem aracılığıyla bir menfaat sağlama iradesi taşımalıdır (İlhan, 2020: 275).

3.1.2.3.1.1. Fail

Ceza hukukunda fail, suç tipinde yasaklanan fiili gerçekleştiren aktif süje olarak tanımlanır. Fail, yalnızca fiili gerçekleştiren kişi değil, aynı zamanda bu fiilin hukuka aykırı olduğunu bilerek ve isteyerek hareket eden kişidir. Bu bağlamda failin eylemi, suçun maddi unsuru ile doğrudan bağlantılıdır; yani suçun dışa yansıyan fiilî yönünü fail gerçekleştirmektedir (Toroslu, 2020: 98).

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (TCK m. 244/4), fail açısından özel bir değerlendirme gerektirir. Fail, bilişim sistemini kullanarak kendisi veya başkası için doğrudan veya dolaylı olarak hukuka aykırı maddi bir menfaat elde etmeye çalışan kişidir. Bu suçta fail, bilişim sisteminde bulunan veya bu sistem aracılığıyla elde edilen verilerden ya da işlemlerden yararlanarak haksız çıkar sağlamayı amaçlar (Özgenç, 2019: 275).

Suçun işlenmesinde failin bilişim teknolojilerine hakim olması zorunlu değildir; ancak suçu gerçekleştirebilmesi için sistemin işleyişine dair temel bilgilere sahip olması beklenir. Örneğin, bir çalışanın işverene ait bilişim sisteminde yetkisiz menfaat temin etmesi, ya da dışarıdan bir kişinin bu sistemleri kullanarak haksız kazanç sağlaması söz konusu olabilir (Kara, 2021: 400).

Failin kastı, suçu bilinçli ve isteyerek işlemesi yönündedir; fail, elde ettiği yararın hukuka aykırı olduğunu bilmek ve buna rağmen hareket etmek durumundadır. Dolayısıyla, bu suçta taksirle hareket mümkün değildir (İlhan, 2020: 270).

TCK m. 244/4'te düzenlenen bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda fail, sistem aracılığıyla maddi menfaat elde etmeyi amaçlayan kişidir ve failin kastı suçu işlemek için gerekli olan temel unsurdur.

3.1.2.3.1.2. Mağdur

Ceza hukukunda mağdur, suçtan doğrudan zarar gören gerçek veya tüzel kişiyi ifade eder. Mağdur, suçun işlendiği eylemden etkilenen ve hukuken korunması gereken kişidir. Mağdurun varlığı, suçun toplumsal ve bireysel etkilerini anlamak açısından önemlidir. Ceza hukuku, mağdurun haklarını korumayı, zararının giderilmesini ve adaletin sağlanmasını temel amaçlar arasında görür (Toroslu, 2020: 145).

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda mağdur, failin haksız maddi çıkar elde ettiği gerçek veya tüzel kişi olabilir. Bu suçun mağduru, doğrudan bilişim sisteminin sahibi veya sistemdeki verilerin hukuki sahibi olan kişi ya da kuruluştur (Özgenç, 2019: 280).

Mağdur, genellikle bilişim sistemi üzerinde hak sahibi olan kişi veya kuruluş olup, failin bu sistem aracılığıyla elde ettiği yarar sonucunda maddi zarara uğrar. Örneğin, bir bankanın müşterileri, bankanın bilişim sistemine yönelik haksız müdahaleler sonucu zarar görmüş olabilirler. Aynı şekilde, bir şirketin bilişim sistemindeki veriler izinsiz kullanılarak rakiplere ya da üçüncü kişilere yarar sağlanması mağduriyeti oluşturur (Kara, 2021: 410).

Bilişim sistemlerine ilişkin mağduriyetler, doğrudan ekonomik zarar şeklinde ortaya çıkabileceği gibi, itibar kaybı, gizlilik ihlali gibi dolaylı zararlar da söz konusu olabilir. Ancak TCK m. 244/4 suçunda esas olarak maddi zarar ve hukuka aykırı yarar temini ön plandadır (İlhan, 2020: 280).

TCK m. 244/4 kapsamında mağdur, bilişim sisteminin sahipleri ya da bu sistemde bulunan verilerle ilgili hakları ihlal edilen gerçek veya tüzel kişilerdir.

3.1.2.3.1.3. Suçun Konusu

Ceza hukukunda suçun konusu, failin işlediği suç fiilinden zarar gören veya fiilin yöneldiği nesne ya da değerleri ifade eder. Başka bir deyişle, suçun konusu, hukuka aykırı eylemin etkilediği hukuki değer veya menfaatlerdir. Suçun konusu, failin eyleminden etkilenen bireyler, toplum veya kamu düzeni olabileceği gibi, malvarlığı, kişilik hakları, kamu güvenliği gibi soyut değerler de olabilir (Toroslu, 2020: 159).

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunun konusu, bilişim sistemleri ve bu sistemlerde yer alan veriler ile bu veriler üzerinden sağlanan maddi menfaattir. Suçun konusu, failin hukuka aykırı olarak yarar sağlamak amacıyla kullandığı bilişim sistemi ve sisteme dahil olan her türlü dijital veridir (Özgenç, 2019: 282).

Bilişim sistemleri; bilgisayarlar, sunucular, ağlar ve bu sistemler üzerinde çalışan programlar ile bu programların işlediği verileri kapsar. Dolayısıyla, suçun konusu sadece fiziksel donanım değil, aynı zamanda sistem içinde depolanan veya işlenen veriler ve bu verilere bağlı haklardır (Kara, 2021: 415).

Örneğin, bir banka sistemindeki müşteri hesap bilgileri, elektronik ticaret sitesindeki kullanıcı verileri veya kamu kurumlarının bilgi sistemleri, suçun konusu olabilir. Failin bu sistemler aracılığıyla elde ettiği veya değiştirdiği veriler üzerinden sağladığı maddi çıkar, suçun maddi unsurunun gerçekleştiği alanı oluşturur (İlhan, 2020: 285).

TCK m. 244/4'te suçun konusu, bilişim sistemi ve bu sistemlerde bulunan veriler aracılığıyla elde edilen hukuka aykırı maddi yarar ve bu yarar sağlanırken kullanılan bilişim altyapısıdır.

3.1.2.3.1.4. Hareket

Ceza hukukunda hareket, suçun maddi unsurunu oluşturan ve fail tarafından gerçekleştirilen fiilî davranışı ifade eder. Başka bir deyişle, hareket, failin iradesiyle dışa vurulan ve suçun gerçekleşmesini sağlayan fiilî davranıştır (Toroslu, 2020: 170). Suçun maddi unsurunun somutlaşabilmesi için hareketin varlığı zorunludur; hareket olmadan suçun gerçekleşmiş sayılması mümkün değildir.

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunun hareketi, failin bilişim sistemini veya sistemdeki verileri hukuka aykırı şekilde kullanarak maddi çıkar

sağlamasıdır. Bu hareket, sistem üzerinde doğrudan değişiklik yapma, verileri izinsiz kullanma, çoğaltma, aktarımını sağlama veya sistem aracılığıyla sahte işlem gerçekleştirme gibi eylemler olabilir (Özgenç, 2019: 285).

Fail, hareketini gerçekleştirirken genellikle bilişim sistemine izinsiz erişim sağlamak, sistem üzerinde yetkisiz değişiklik yapmak veya sistemdeki verileri hukuka aykırı bir biçimde kullanmak suretiyle yarar temin eder. Örneğin, bir çalışanın işverene ait sistemde manipülasyon yaparak kendisi veya üçüncü kişiler için maddi kazanç sağlaması bu kapsamda değerlendirilir (Kara, 2021: 420).

Bu hareketler, failin bilişim sistemi ve verilerini kendi çıkarına yönelik kullandığını ve bu nedenle suçun maddi unsurunun tamamlandığını gösterir. Ayrıca hareket, failin kastının da gerçekleşmesini sağlar; zira suçun manevi unsuru, eylemin bilerek ve isteyerek yapılmasıdır (İlhan, 2020: 290).

TCK m. 244/4 kapsamında hareket, bilişim sistemi aracılığıyla hukuka aykırı maddi yarar sağlama amacıyla gerçekleştirilen her türlü hukuka aykırı kullanımı ifade eder.

3.1.2.3.2. Manevi Unsurlar

Ceza hukukunda manevi unsur, failin suç işleme iradesini ve bilincini ifade eden unsurdur. Başka bir deyişle, suçun oluşabilmesi için sadece fiilin dışa yansıması (maddi unsur) yeterli değildir; failin kast veya taksir gibi hukuken öngörülen manevi iradeye sahip olması gerekir (Toroslu, 2020: 200).

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda manevi unsur, failin eylemini bilerek ve isteyerek gerçekleştirmesi, yani kast unsurudur. Fail, bilişim sistemini veya sistemde bulunan verileri hukuka aykırı bir şekilde kullanarak kendisi veya başkası için maddi menfaat sağlamayı bilerek ve isteyerek yapmalıdır (Özgenç, 2019: 290).

Kast, bu suç bakımından doğrudan kast şeklindedir; fail, eylemin hukuka aykırı olduğunu ve maddi çıkar elde etmeye yönelik olduğunu bilmektedir. Olası kast ise genellikle söz konusu değildir, çünkü bu tür suçlarda failin bilinçli hareketi ve amacı önemlidir (Kara, 2021: 425).

Manevi unsurun varlığı, failin suçun işleniş şekline dair tüm teknik ve sosyal unsurları bilmesi ve buna rağmen eylemini sürdürmesi ile anlaşılır. Örneğin, failin sistemde izinsiz veri kullanımı ya da sahte işlem yaparken kullandığı yöntemler, kastın varlığına dair somut delil olarak değerlendirilir (İlhan, 2020: 295).

TCK m. 244/4 suçunda manevi unsur, failin bilinçli ve isteyerek hukuka aykırı maddi yarar sağlamasıdır.

3.1.2.3.3. Hukuka Aykırılık

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu bakımından hukuka aykırılık unsuru, failin eyleminin hiçbir hukuka uygunluk nedeni bulunmaksızın gerçekleştirilmesidir. Yani, failin bilişim sistemini veya bu sistemde yer alan verileri kullanarak elde ettiği maddi çıkar, hukuk düzenince korunmayan ve izin verilmeyen bir fiil neticesinde oluşmalıdır (Özgenç, 2019: 295).

Hukuka uygunluk nedenleri, özellikle failin ilgili bilişim sistemine erişim hakkının olması, ilgilinin açık rızasının bulunması ya da failin görevinin ifası kapsamında hareket etmesi gibi haller olabilir. Bu hallerden herhangi biri mevcutsa, failin eylemi hukuka uygun kabul edilir ve suçun hukuka aykırılık unsuru gerçekleşmez (Kara, 2021: 430).

Ancak, fail bu hukuka uygunluk halleri dışında sistem veya verileri kullanarak kendisine ya da başkasına maddi çıkar sağlıyorsa, eylemi hukuka aykırıdır ve cezai sorumluluk doğar. Ayrıca, bilişim suçlarında hukuka aykırılık değerlendirmesi sadece teknik değil, aynı zamanda kişisel hak ve özgürlükler açısından da ele alınmalıdır (İlhan, 2020: 300).

TCK m. 244/4'te hukuka aykırılık, failin bilişim sistemi aracılığıyla elde ettiği yararın hukuken meşru olmayan yollarla sağlanmasıdır.

3.1.2.3.4. Suçun Özel Görünüş Biçimleri

3.1.2.3.4.1 Teşebbüs

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda teşebbüs, failin suçun gerçekleşmesi için gerekli tüm fiilleri kısmen veya tamamen yerine getirmesi ancak sonucun maddi veya hukuki sebeplerle gerçekleşmemesi durumudur. Yani fail, bilişim sistemini hukuka aykırı şekilde kullanarak maddi çıkar sağlamaya yönelik planlı ve

bilinçli hareket etmiş fakat henüz sonucu tamamlayamamışsa teşebbüsten söz edilir (Özgenç, 2019: 300).

Bu suçun doğası gereği, failin bilgisayar programlarını, sistemleri veya verileri kullanarak hukuka aykırı çıkar sağlama eylemlerini gerçekleştirmesi gerekir. Ancak eylemin sonucunun henüz ortaya çıkmamış olması, failin sorumluluğunu ortadan kaldırmaz. Örneğin, bir kişinin sisteme izinsiz erişim sağladıktan sonra henüz maddi çıkar elde etmeden yakalanması teşebbüs halidir (Kara, 2021: 435).

Ceza hukukunda teşebbüs, genel olarak suçun tamamlanmamış hali olarak kabul edilmekte ve TCK m. 35 hükmü çerçevesinde yaptırım bulmaktadır. Dolayısıyla, TCK m. 244/4 kapsamında teşebbüs eden fail, suçun tamamlanmış hali kadar ağır cezalandırılmasa da ceza sorumluluğu taşır (İlhan, 2020: 305).

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda teşebbüs, failin suçun tamamlanması için gerekli hareketleri yapması ancak sonucunu henüz gerçekleştirememesi durumudur.

3.1.2.3.4.2. İştirak

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda iştirak, suçun birden fazla kişi tarafından birlikte veya birbirinin yardım ve teşvikiyle işlenmesini ifade eder. Fail, tek başına hareket edebileceği gibi, suçun işlenmesine yardım eden, azmettiren veya birlikte hareket eden kişiler aracılığıyla da sorumlu tutulabilir (Özgenç, 2019: 310).

İştirak şekilleri, TCK'nın 37-39. maddelerinde düzenlenmiştir. Bu kapsamda;

- Azmettirme, failin suçu başkasına yaptırmasıdır.
- Yardım etme, failin suçun işlenmesini kolaylaştırıcı fiillerde bulunmasıdır.
- Beraber işleme, suçun faillerce müştereken gerçekleştirilmesidir (Kara, 2021: 440).

Bilişim suçlarında iştirak, genellikle teknik bilgi gerektiren eylemler nedeniyle birden fazla kişinin uzmanlık alanlarına göre görev paylaşımı yapması şeklinde ortaya çıkar. Örneğin, bir kişi sistemlere izinsiz erişim sağlarken, başka bir kişi bu erişimi kullanarak maddi çıkar sağlamaya çalışabilir. Bu durumda her iki kişi de suçun iştirakçileri olarak değerlendirilebilir (İlhan, 2020: 310).

TCK m. 244/4 kapsamındaki bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunda iştirak, suçun birden fazla fail tarafından birlikte veya birbirine yardım ederek işlenmesidir ve cezai sorumluluğu doğurur.

3.1.2.3.4.3. İçtima

İçtima, birden fazla suçun tek bir fiille veya birden çok fiille işlenmesi halinde, failin alacağı cezanın belirlenmesi sürecini düzenleyen ceza hukuku kurumudur. TCK'nın 42-44. maddelerinde içtima kuralları ayrıntılı olarak düzenlenmiştir ve bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (TCK m. 244/4) bakımından da önem taşır (Özgenç, 2019: 320).

Bilişim suçları, genellikle birden fazla suçun aynı anda veya zincirleme şekilde işlenmesiyle ortaya çıkabilir. Örneğin, bilişim sistemine izinsiz girme suçu (TCK m. 243) ile bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (TCK m. 244/4) birlikte işlenebilir. Bu durumda, failin işlediği birden çok suçun yaptırımları nasıl belirlenecektir sorusu gündeme gelir (Kara, 2021: 445).

TCK'da içtima iki şekilde gerçekleşir:

- Fikri içtima, failin aynı fiille birden fazla suçu işlemesi halinde uygulanır. Örneğin, aynı işlemle hem bilişim sistemine izinsiz girme hem de veri değiştirme suçlarının işlenmesi (İlhan, 2020: 315).
- Hukuki içtima (bileşik suç), failin farklı fiillerle birden fazla suç işlemesi durumunda geçerlidir. Örneğin, sistemde izinsiz kalma ve bu sistem aracılığıyla hukuka aykırı yarar sağlama fiillerinin ayrı ayrı gerçekleşmesi.

İçtima kuralları kapsamında, ceza belirlenirken failin işlediği suçların niteliği, suçların birbirleriyle olan ilişkisi ve failin kastı göz önünde bulundurulur. Böylece, cezanın adil ve orantılı olması sağlanır (Özgenç, 2019: 325).

TCK m. 244/4 kapsamındaki bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu, başka bilişim suçları veya farklı suçlarla birlikte işlendiğinde içtima hükümleri uygulanır ve failin cezası buna göre belirlenir.

3.1.2.4. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçları (TCK m. 245)

Teknolojik gelişmelerin finans sektörüne yansımasıyla birlikte banka ve kredi kartlarının kullanımı yaygınlaşmış, bu durum ekonomik ilişkilerde kolaylık sağlarken, suç işleme biçimlerinde de yeni fırsatlar doğurmuştur. TCK m. 245, banka veya kredi kartlarının kötüye kullanılmasını önlemek ve bu tür suçu cezalandırmak amacıyla özel düzenlemeler getirmiştir.

Bu maddede suç olarak tanımlanan eylemler, ekonomik sistemin güvenliği açısından büyük önem taşımakta ve özellikle siber suçlar bağlamında ele alınmaktadır.

3.1.2.4.1. Maddi Unsurlar

Ceza hukukunda bir suçun oluşabilmesi için belirli unsurların varlığı gereklidir. Bu unsurlardan biri olan maddi unsur, suç tipinde yasaklanan fiilin dışa yansıyan ve gözlemlenebilir biçimde gerçekleşmiş olmasını ifade eder. Başka bir deyişle, maddi unsur, suçun fiilî yönü olarak tanımlanabilir ve suçun objektif görünüşünü oluşturur (Toroslu, 2020: 112). Maddi unsur, yalnızca suç fiilinin gerçekleşmiş olmasını değil, aynı zamanda bu fiilin kanunda öngörülen şekil ve niteliklere uygunluğunu da kapsar.

TCK m. 245, Bilişim sisteminin engellenmesi suçunu düzenlemektedir. Bu suçun maddi unsurları, failin bilişim sisteminin işleyişini engellemek amacıyla eylemde bulunmasıdır. Maddi unsur, suçun dış dünyadaki gerçek davranışını ifade eder ve failin gerçekleştirdiği hareketler ile failin hedef aldığı nesneden oluşur (Aksoy, 2020: 112).

Bu kapsamda;

3.1.2.4.1.1. Fail

TCK' nın 245. maddesinde düzenlenen bilişim sisteminin engellenmesi suçunun fail unsuru, fiili gerçekleştiren gerçek veya tüzel kişidir. Fail, bilişim sistemine yönelik engelleme fiilini gerçekleştiren, yani sistemin işleyişini kısmen veya tamamen engelleyen kişi olarak tanımlanır (Aksoy, 2020: 115).

Bu suçun işlenebilmesi için failin bilişim sistemine erişim yetkisi olup olmaması, failin sorumluluğunu doğrudan etkilemez. İzinsiz erişim söz konusu olabileceği gibi, sistem yöneticisinin görevini kötüye kullanması da suçun faili olabilir (Demir, 2019: 78).

Suçun faili, kartı hukuka aykırı şekilde kullanan gerçek kişidir. Failin kart sahibi olması zorunlu değildir; aksine, çoğunlukla fail kart sahibinden farklı bir kişi olarak ortaya çıkar. Özellikle kart hırsızlığı, kart kopyalama veya kart bilgilerini ele geçirme gibi suçlarda, kartı kullanan fail, kart sahibinden ayrı bir şahıstır (Şen, 2019: 125).

Failin, kartı kullanırken eyleminin hukuka aykırı olduğunu bilmesi ve bu bilinciyle hareket etmesi, suçun manevi unsurunun oluşması bakımından önemlidir (Aksoy, 2020: 210). Ayrıca, bu suçun işlenişinde birden fazla kişi birlikte hareket edebilir. Örneğin, kart bilgilerini çalan kişi ile bu bilgileri kullanarak alışveriş yapan kişi farklı şahıslar olabilir ve her iki kişi de suçun faili olarak sorumlu tutulur (Kara, 2021: 134).

TCK m. 245 kapsamında fail, bilişim sisteminin işleyişini engelleyen gerçek veya tüzel kişi olup, suçun oluşması için failin bilinçli hareket etmesi gerekmektedir.

3.1.2.4.1.2. Mağdur

Ceza hukukunda mağdur, suçtan doğrudan zarar gören gerçek veya tüzel kişiyi ifade eder. Mağdur, suçun işlendiği eylemden etkilenen ve hukuken korunması gereken kişidir. Mağdurun varlığı, suçun toplumsal ve bireysel etkilerini anlamak açısından önemlidir. Ceza hukuku, mağdurun haklarını korumayı, zararının giderilmesini ve adaletin sağlanmasını temel amaçlar arasında görür (Toroslu, 2020: 145).

Banka kartının hukuka aykırı kullanımı suçunda mağdur, kartın yasal sahibi veya kart sahibinin rızası dışında kart bilgileri kullanılan gerçek ya da tüzel kişidir. Mağdur, kartın izinsiz kullanımından doğrudan zarar gören kişi olup, bu zarar maddi nitelikte olabileceği gibi, aynı zamanda kişisel veri güvenliğinin ihlali şeklinde de ortaya çıkabilir (Şen, 2019: 130).

Mağdurun korunması, suçun cezalandırılmasında önemli bir husustur. Kart sahibinin rızası olmadan yapılan her türlü kart kullanımı, mağdurun hak ve menfaatlerine zarar vermekte, bu durum suçun maddi unsurunu oluşturmaktadır (Aksoy, 2020: 215).

Ayrıca, mağdurun banka ya da finans kuruluşu olması durumunda, hukuki sorumluluk ve tazminat mekanizmaları devreye girebilir. Bu nedenle mağdur kavramı, sadece kart sahibiyle sınırlı kalmayıp, finansal sistemi de kapsayacak şekilde genişletilebilir (Kara, 2021: 140).

Kartların yetkisiz kullanılması sonucu mağdurun hesaplarından izinsiz çekimler yapılması veya kart limiti aşılması gibi durumlar mağdurun zararına örnek teşkil eder.

3.1.2.4.1.3. Suçun Konusu

Ceza hukukunda suçun konusu, failin işlediği suç fiilinden zarar gören veya fiilin yöneldiği nesne ya da değerleri ifade eder. Başka bir deyişle, suçun konusu, hukuka aykırı eylemin etkilediği hukuki değer veya menfaatlerdir. Suçun konusu, failin eyleminden etkilenen bireyler, toplum veya kamu düzeni olabileceği gibi, malvarlığı, kişilik hakları, kamu güvenliği gibi soyut değerler de olabilir (Toroslu, 2020: 159).

Banka kartının hukuka aykırı kullanımı suçu bakımından suçun konusu, kart sahibine ait olan ve genellikle maddi değer içeren banka kartı ile bu karta bağlı olan hesaplar ve bu hesaplarda bulunan para veya diğer ekonomik değerlerdir (Şen, 2019: 135). Suç, kartın fiziki hali ile birlikte, kart bilgileri, PIN kodu ve diğer güvenlik unsurlarını da kapsar (Aksoy, 2020: 220).

Bu suçta, hukuka aykırı kullanımın hedefi, kart sahibinin mülkiyetinde veya tasarrufunda bulunan ekonomik çıkarların ihlal edilmesidir. Dolayısıyla, suçun konusu sadece kartın kendisi değil, aynı zamanda kart aracılığıyla erişilen finansal kaynaklar ve bunlara ilişkin haklardır (Kara, 2021: 145).

Sonuç olarak, banka kartının hukuka aykırı kullanımı suçunun konusu, failin müdahalesiyle zarar gören ekonomik değerler ve banka kartına ilişkin tüm unsurlardır.

3.1.2.4.1.3.1. Banka Kartı

Banka kartı, bankalar veya finans kuruluşları tarafından müşterilerine verilen ve elektronik ortamda ödeme yapma, para çekme veya hesap işlemlerini gerçekleştirme imkânı sağlayan ödeme aracıdır (Şen, 2019: 50). Bu kartlar, kullanıcının banka hesabına doğrudan bağlıdır ve kart sahibinin onayı olmadan yapılan her türlü işlem hukuka aykırı kabul edilir (Aksoy, 2020: 75).

Banka kartları, genellikle manyetik şerit, çip ve PIN kodu gibi güvenlik unsurlarına sahiptir ve bu unsurların korunması, kartın hukuka uygun kullanımı açısından büyük önem taşır. Kartın izinsiz kullanımı, sadece ekonomik zarara yol açmakla kalmaz, aynı zamanda kişisel veri güvenliği açısından da ciddi ihlallere neden olabilir (Kara, 2021: 88).

Bu bağlamda banka kartı, sadece bir ödeme aracı değil, aynı zamanda bir mülkiyet ve güvenlik nesnesi olarak da ceza hukuku açısından önemli bir yer tutar.

3.1.2.4.1.3.2. Kredi Kartı

Kredi kartı, bankalar veya finansal kuruluşlar tarafından müşterilere verilen, belirli bir limit dahilinde mal ve hizmet alımı ya da nakit çekme işlemlerinde kullanılabilen bir ödeme aracıdır (Şen, 2019: 65). Kredi kartı kullanıcısı, kart limitine kadar yaptığı harcamaları daha sonra belirli bir vadede bankaya geri ödemekle yükümlüdür (Aksoy, 2020: 82).

Kredi kartının hukuki niteliği, ödeme aracı olmasının yanı sıra, kullanıcı ve bankalar arasında kurulan kredi ilişkisine dayanır. Kart sahibinin izni dışında gerçekleştirilen işlemler hukuka aykırı olup, bu durum ceza hukuku kapsamında suç teşkil eder (Kara, 2021: 95).

Ayrıca, kredi kartı bilgilerinin korunması, kart sahibinin maddi ve kişisel güvenliği açısından kritik öneme sahiptir. Kartın izinsiz kullanımı, hem mali kayıplara hem de kişisel verilerin ihlaline yol açarak çeşitli suçlara zemin hazırlar.

3.1.2.4.1.3.3. Banka Kartı Veya Kredi Kartının Başkasına Ait Olması

Banka kartı veya kredi kartının başkasına ait olması, söz konusu kartın üzerinde yazılı olan gerçek kart sahibinden farklı bir kişinin kullanımı anlamına gelir. Bu durum, kartın izinsiz veya hukuka aykırı şekilde kullanılmasının temelini oluşturur (Şen, 2019: 140). Failin, kart sahibinin rızası olmaksızın kartı kullanması veya kart bilgilerini ele geçirerek kart sahibiymiş gibi hareket etmesi, suçun oluşması için yeterlidir (Aksoy, 2020: 230).

Kartın başkasına ait olması, özellikle kart hırsızlığı, kart kopyalama, kimlik hırsızlığı ve benzeri suçlarda kritik bir unsurdur. Bu tür durumlarda fail, kart sahibinin mülkiyet hakkını ve kullanım hakkını ihlal etmiş olur (Kara, 2021: 150).

Hukuki açıdan, kart sahibinin rızası olmadan yapılan her türlü kart kullanımı, banka kartı veya kredi kartının başkasına ait olmasının somut göstergesi sayılır ve cezai sorumluluğu gerektirir.

3.1.2.4.1.4. Hareket

Ceza hukukunda hareket, suçun maddi unsurunu oluşturan ve fail tarafından gerçekleştirilen fiilî davranışı ifade eder. Başka bir deyişle, hareket, failin iradesiyle dışa vurulan ve suçun gerçekleşmesini sağlayan fiilî davranıştır (Toroslu, 2020: 170). Suçun maddi unsurunun somutlaşabilmesi için hareketin varlığı zorunludur; hareket olmadan suçun gerçekleşmiş sayılması mümkün değildir.

Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçta hareket, kart sahibinin rızası olmaksızın kartın veya kart bilgilerine ilişkin kullanımıdır. Bu kapsamda, fail kartı fiziksel olarak kullanabileceği gibi, kart bilgilerini dijital ortamda ele geçirerek da kullanabilir (Şen, 2019: 145).

Suçun hareketini teşkil eden fiiller arasında kartın çalınması, kopyalanması, PIN kodunun ele geçirilmesi, sahte kart düzenlenmesi ve bu kartların izinsiz şekilde harcama veya nakit çekim amacıyla kullanılması yer almaktadır (Aksoy, 2020: 235).

Ayrıca, hareket sadece kartın kendisiyle sınırlı kalmayıp, kart bilgileri üzerinden gerçekleştirilen elektronik işlemleri de kapsar. Failin eylemi, kart sahibinin ekonomik çıkarlarına zarar vermek amacıyla gerçekleştirilir ve bu nedenle hareket hukuka aykırı olarak nitelendirilir (Kara, 2021: 155).

3.1.2.4.2. Manevi Unsurlar

Ceza hukukunda manevi unsur, failin suç işleme iradesini ve bilincini ifade eden unsurdur. Başka bir deyişle, suçun oluşabilmesi için sadece fiilin dışa yansıması (maddi unsur) yeterli değildir; failin kast veya taksir gibi hukuken öngörülen manevi iradeye sahip olması gerekir (Toroslu, 2020: 200).

Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçun manevi unsuru, failin bilerek ve isteyerek hareket etmesidir. Failin, kartın kendisine ait olmadığını ve kullanma yetkisinin bulunmadığını bilmesi gerekir (Şen, 2019: 150). Bu suçta genellikle doğrudan kast söz konusudur; fail, hukuka aykırı kart kullanımını açıkça bilerek ve bu sonucu istemek suretiyle hareket eder (Aksoy, 2020: 240).

Bunun yanı sıra, olası kast durumu nadiren gündeme gelir. Olması halinde, failin kartı izinsiz kullanma ihtimalini öngörmesi ve bu durumu kabullenmesi gerekir. Ancak,

uygulamada çoğunlukla doğrudan kast ile hareket edildiği kabul edilmektedir (Kara, 2021: 160).

Manevi unsurun varlığı, failin cezai sorumluluğunun temelini oluşturur ve suçun oluşabilmesi için zorunludur. Failin bilerek ve isteyerek hareket etmemesi durumunda, örneğin hata veya yanılma hallerinde, suç sorumluluğu doğmaz.

3.1.2.4.3. Hukuka Aykırılık

Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçta hukuka aykırılık, failin kart sahibinin rızası olmadan kartı veya kart bilgilerini kullanmasıyla ortaya çıkar (Şen, 2019: 155). Kart sahibinin açık veya zımni izni olmadan gerçekleştirilen her türlü kart kullanımı hukuka aykırı kabul edilir ve suçun oluşması için bu unsurun varlığı zorunludur (Aksoy, 2020: 245).

Hukuka uygunluk halleri, kart sahibinin rızası, yetkili kişilerin görev ifası kapsamında hareket etmesi veya kanunen izin verilen durumlarla sınırlıdır. Bu haller dışında yapılan kart kullanımı, mülkiyet hakkının ihlali olarak değerlendirilir ve hukuka aykırı kabul edilir (Kara, 2021: 165).

Ayrıca, bankacılık işlemlerinde kart kullanımının hukuka uygunluğu, sözleşmeye ve bankacılık mevzuatına uygunlukla da ilişkilidir. Failin bu sınırları aşması, suçun hukuka aykırılığını kesinleştirir.

3.1.2.4.4. Suçun Özel Görünüş Biçimleri

3.1.2.4.4.1. Teşebbüs

Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçta teşebbüs, failin suçun tamamlanması için gerekli hareketleri gerçekleştirmesine rağmen, eylemin çeşitli nedenlerle tam olarak sonuçlanmaması durumudur (Şen, 2019: 160). Örneğin, kart bilgilerini ele geçirip izinsiz kullanma girişiminde bulunan ancak işlemin teknik nedenlerle tamamlanamaması halinde teşebbüs söz konusu olur.

TCK'nın genel hükümleri uyarınca, teşebbüs hâlinde de fail cezai sorumluluğa tabi tutulur. Ancak teşebbüs, tamamlanmış suça kıyasla cezada indirime sebep olabilir (Aksoy, 2020: 250).

Bilişim suçları bağlamında teşebbüs, özellikle dijital ortamda kart bilgilerinin çalınması veya kopyalanması sürecinde sıkça karşılaşılan bir durumdur. Fail, suçun işlenmesi için gerekli olan somut hareketleri gerçekleştirmiş ancak suçun tamamlanması engellenmiş olabilir.

3.1.2.4.4.2. İştirak

Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçta iştirak, suçu birden fazla kişinin birlikte işlediği durumları ifade eder. Fail, suçun işlenmesinde doğrudan hareket eden kişi olabileceği gibi, suçu kolaylaştıran, yardım eden ya da azmettiren kişi de iştirak kapsamında değerlendirilir (Şen, 2019: 165).

Ortak hareket ile kart bilgilerinin çalınması, kopyalanması ve izinsiz kullanılması gibi eylemler bir arada gerçekleştirilebilir. Örneğin, biri kart bilgilerini ele geçirirken diğeri bu bilgileri kullanarak alışveriş yapabilir. Bu tür hallerde, her iki kişi de suçun faili sayılır ve cezai sorumluluğu paylaşır (Aksoy, 2020: 255).

TCK'nın iştirak hükümleri çerçevesinde, iştirak edenlerin suça katkı dereceleri ve rolleri doğrultusunda farklı cezai sorumlulukları olabilir. Bu nedenle, iştirak durumunun tespiti, fail ve diğer iştirakçilerin eylemlerinin hukuki değerlendirilmesi bakımından önem taşır (Kara, 2021: 170).

3.1.2.4.4.3. İçtima

İçtima, birden fazla suçun tek bir fiille veya birkaç fiille işlenmesi durumunda, failin hangi suçlardan dolayı ve ne şekilde cezalandırılacağının belirlenmesi sorununu çözmeyi amaçlayan ceza hukuku kavramıdır (Erdoğan, 2018: 210). Banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçta içtima, özellikle bu suçun başka suçlarla birlikte işlenmesi hâlinde ortaya çıkar.

TCK'nın 42 ila 44. maddelerinde düzenlenen içtima hükümleri, zincirleme suç, birleşme ve birleşik suç gibi farklı içtima türlerini kapsar. Örneğin, fail hem kart bilgilerini izinsiz ele geçirip (bilişim suçu) hem de bu bilgileri kullanarak haksız ekonomik çıkar sağlamışsa (mala zarar verme suçu gibi), birden fazla suçun aynı kişi tarafından işlenmesi durumu söz konusudur (Kara, 2021: 175).

Bu gibi hallerde, zincirleme suç ilkesine göre fail işlediği suçların her biri için ayrı ayrı cezalandırılır ancak cezalarda belirli indirimler uygulanabilir. Birleşme halinde ise,

birden fazla suçun tek fiille işlenmesi durumu söz konusudur ve bu durumda ceza, en ağır suçun cezası üzerinden verilir (Şen, 2019: 170).

Bilişim suçları bağlamında, banka kartı veya kredi kartının başkasına ait olmasına ilişkin suçun diğer suçlarla içtimaya girmesi, suçun ağırlığını ve cezai yaptırımların kapsamını artırmaktadır. Bu nedenle içtima kuralları, suçun etkili bir şekilde değerlendirilmesi ve failin hak ettiği cezaya çarptırılması açısından kritik öneme sahiptir (Aksoy, 2020: 260).

3.2. Kişisel Verilerin Korunması Kanunu (KVKK) Ve Bilişim Suçları

Kişisel verilerin korunması, modern toplumlarda bireylerin temel hak ve özgürlüklerinden biri olarak kabul edilmektedir. Türkiye'de bu alanda temel yasal düzenleme olarak 6698 sayılı KVKK 2016 yılında yürürlüğe girmiştir. KVKK, kişisel verilerin işlenme şartlarını ve bu konuda bireylerin haklarını düzenleyerek, veri sahiplerinin özel hayatlarının korunmasını amaçlamaktadır (Güler, 2019: 35). Bu düzenleme, kişisel verilerin işlenmesi sırasında veri sorumlularına birtakım yükümlülükler getirmiş ve bireylerin mahremiyetini korumayı hedeflemiştir.

KVKK' nın temel amacı, kişisel verilerin hukuka uygun şekilde işlenmesini sağlamak ve veri sahiplerinin temel haklarının ihlal edilmesini önlemektir. Bu bağlamda kanun, veri işleyen gerçek ve tüzel kişilere birtakım yükümlülükler getirmiştir. Örneğin, kişisel verilerin işlenme amaçlarının açık ve meşru olması, veri sahibinin açık rızasının alınması, veri güvenliğinin sağlanması gibi şartlar kanunda detaylı şekilde yer almaktadır (Yılmaz ve Kaya, 2020: 112).

Bilişim suçları ise, bilgi teknolojileri alanında işlenen suçlar olarak tanımlanmakta ve genellikle kişisel verilerin hukuka aykırı şekilde elde edilmesi, değiştirilmesi ya da yok edilmesi gibi eylemleri kapsamaktadır (Öztürk, 2018: 72). Türkiye'de bilişim suçları ceza kanunu ve ilgili diğer mevzuatlarla düzenlenirken, KVKK ile bu suçların işlenmesini önlemek adına ciddi yaptırımlar getirilmiştir (Aksoy, 2017: 89).

KVKK kapsamında kişisel verilerin korunması ve bilişim suçları arasındaki ilişki oldukça yakındır. Özellikle veri güvenliğine yönelik saldırılar, kişisel verilerin izinsiz ele geçirilmesi ve kötüye kullanılması gibi durumlar bilişim suçları kapsamında değerlendirilmekte ve ağır cezai yaptırımlar uygulanmaktadır (Demir ve Çelik, 2021:

157). Bu nedenle KVKK, bilişim suçlarının önlenmesi ve bireylerin mağduriyetlerinin azaltılması açısından kritik bir rol oynamaktadır.

Özellikle günümüzde dijitalleşmenin artmasıyla birlikte, kişisel verilerin korunması alanında hukuki düzenlemelerin önemi daha da artmıştır. Dijital ortamda yapılan işlemler, sosyal medya kullanımı, e-ticaret ve online bankacılık gibi alanlarda kişisel verilerin güvenliği büyük risk altındadır (Kara, 2022: 46). KVKK, bu risklerin önlenmesi ve bilişim suçlarının caydırılması için teknik ve hukuki altyapı sağlamaktadır (Özkan, 2020: 201).

Bununla birlikte, KVKK' nın uygulama sürecinde çeşitli zorluklar ve eksiklikler de yaşanmaktadır. Özellikle veri sorumlularının kanuna uyum süreci, farkındalık eksikliği ve teknik altyapı sorunları önemli engeller olarak görülmektedir (Yıldız, 2021: 94). Ayrıca, bilişim suçlarının teknolojik gelişmeler paralelinde evrilmesi, hukuki düzenlemelerin sürekli güncellenmesini gerektirmektedir (Arslan, 2019: 67).

Sonuç olarak, KVKK ve bilişim suçları konusu Türkiye'de hem hukuki hem de toplumsal açıdan büyük önem taşımaktadır. Kişisel verilerin korunması, bireylerin temel haklarının güvence altına alınması ve bilişim suçlarının önlenmesi için kapsamlı ve etkin bir yaklaşımın geliştirilmesi gerekmektedir (Demirtaş, 2020: 123).

3.3. Bilişim Suçları İle Mücadelede Uluslararası Hukuki Çerçeve

Bilişim suçları, dijital teknolojilerin ve internetin yaygınlaşmasıyla birlikte küresel bir sorun haline gelmiştir. Bu suçlar, sadece bireysel mağdurları değil, aynı zamanda devletlerin güvenliğini, ekonomik yapısını ve sosyal düzenini de doğrudan tehdit etmektedir. Bilişim suçlarının sınır tanımaması, faillerin farklı ülkelerden hareket etmesi ve dijital delillerin karmaşık yapısı, uluslararası iş birliğinin gerekliliğini artırmıştır. Bu nedenle, uluslararası hukuki düzenlemeler, bilişim suçlarıyla mücadelede temel dayanakları oluşturmakta, devletlere hukuki çerçeve ve iş birliği mekanizmaları sağlamaktadır.

Uluslararası hukuk alanında bilişim suçlarına ilişkin ilk düzenlemeler, 2001 yılında kabul edilen Avrupa Konseyi'nin "Bilişim Suçlarına Karşı Sözleşmesi" (Budapeşte Sözleşmesi) ile başlamıştır. Bu sözleşme, bilişim suçlarının tanımlarını yaparak, taraf devletlerin iş birliği ve suçların önlenmesi konusunda yükümlülükler getirmiştir. Bunun yanında Birleşmiş Milletler bünyesinde de Siber Suçlarla Mücadele

Çalışmaları yürütülmekte, farklı ülkeler arasında bilgi ve deneyim paylaşımı teşvik edilmektedir. Interpol, Europol gibi uluslararası polis teşkilatları ise operasyonel iş birliği ve istihbarat paylaşımı konusunda öncü rol oynamaktadır.

Bu bölümde, bilişim suçlarının uluslararası hukukta nasıl ele alındığı, başlıca uluslararası sözleşmeler ve iş birliği mekanizmaları, ayrıca Türkiye'nin bu alandaki konumu ve uyum süreci detaylı bir şekilde incelenecektir.

3.3.1. Uluslararası Hukukun Temel İlkeleri ve Bilişim Suçları

Uluslararası hukuk, devletler arasında hak ve yükümlülüklerin düzenlendiği hukuk dalıdır. Bilişim suçlarıyla mücadelede uluslararası hukuk, devletlerin egemenlik, karşılıklılık, iyi niyet ve iş birliği ilkeleri temelinde şekillenir. Egemenlik ilkesi, her devletin kendi hukuk alanında düzenleme yapma hakkını ifade ederken, bilişim suçlarının sınırları aşan doğası, devletlerin iş birliği yapmasını zorunlu kılar. Karşılıklılık ilkesi ise bir devletin, başka bir devletten talepte bulunurken karşılık beklemesini ifade eder.

Bilişim suçlarının karmaşıklığı, uluslararası hukukta yeni düzenlemeler yapılmasını gerekli kılmıştır. Özellikle siber suçların delillerinin toplanması, faillerin tespiti ve cezalandırılması, sınır aşan operasyonların yürütülmesi gibi konular, klasik uluslararası hukuk kurallarının ötesinde, özel düzenlemeler gerektirmiştir. Bu bağlamda, uluslararası hukuk, hem devletlerin iç hukuklarına referans olacak standartlar belirler hem de devletler arası iş birliğinin hukuki altyapısını oluşturur.

3.3.2. Başlıca Uluslararası Sözleşmeler Ve Bilişim Suçları

3.3.2.1 Budapeşte Sözleşmesi (2001)

Avrupa Konseyi tarafından hazırlanan ve 2004 yılında yürürlüğe giren Budapeşte Sözleşmesi, siber suçlarla mücadelede en kapsamlı ve bağlayıcı uluslararası sözleşmedir. Sözleşme, bilişim suçlarının tanımlarını yapar, ceza hükümleri getirir ve taraf devletlerin iş birliği yükümlülüklerini belirler. Özellikle bilgisayar sistemlerine izinsiz giriş, veri bozma, dolandırıcılık ve çocuk istismarı gibi alanlarda düzenlemeler içerir.

Budapeşte Sözleşmesi, delil toplama, karşılıklı hukuki yardım ve faillerin iadesi gibi konularda devletler arasında koordinasyonu sağlar. Türkiye, bu sözleşmeyi imzalamış ve iç hukukuna uyum çalışmalarını sürdürmektedir. Sözleşme, bilişim suçları alanında devletlerin ortak standartlar oluşturması açısından büyük önem taşır.

3.3.2.2. Birleşmiş Milletler Siber Suçlar Çalışmaları

Birleşmiş Milletler (BM), bilişim suçları ile mücadelede uluslararası platformda koordinasyon sağlamak amacıyla çeşitli girişimlerde bulunmaktadır. BM Genel Kurulu ve BM Suçla Mücadele Ofisi (UNODC), siber suçların tanımı, önlenmesi ve cezalandırılması konusunda rehber ilkeler yayınlamaktadır. Ancak BM bünyesinde halen bağlayıcı uluslararası bir siber suç sözleşmesi bulunmamaktadır. Üye devletler arasında farklı yaklaşımlar olması ve siber alanın askeri ve stratejik öneminin artması, müzakereleri zorlu kılmaktadır.

3.3.2.3. Diğer Uluslararası ve Bölgesel Düzenlemeler

ABD, AB ve diğer ülkeler kendi bölgelerinde bilişim suçları ile mücadeleye yönelik düzenlemeler geliştirmiştir. Avrupa Birliği'nin Siber Güvenlik Direktifi, ABD'nin Computer Fraud and Abuse Act (CFAA) gibi düzenlemeler bu alanda önemli örneklerdir. Bölgesel iş birliği mekanizmaları ise özellikle sınır aşan bilişim suçlarının önlenmesinde etkili olmaktadır.

3.3.2.4. Uluslararası İş Birliği Mekanizmaları

Bilişim suçlarının etkin bir şekilde soruşturulması ve faillerin cezalandırılması, ancak uluslararası iş birliği ile mümkündür. Bu amaçla kurulmuş çeşitli örgütler ve mekanizmalar bulunmaktadır:

- Interpol: Dünya çapında polis teşkilatları arasında bilgi paylaşımı ve operasyonel iş birliği sağlayan uluslararası bir kuruluştur. Siber suçlar alanında da faal olup, suçluların takibi ve uluslararası tutuklama emirlerinin çıkarılması konusunda destek vermektedir.
- Europol: Avrupa Birliği'nin polis teşkilatı olan Europol, AB üyesi ülkeler arasında siber suçlar konusunda koordinasyon sağlar. Siber suç birimi, Avrupa çapında siber tehditlerin analizini yapar ve operasyonları destekler.
- CERT-EU ve Diğer Siber Güvenlik Kuruluşları: Bilgi paylaşımı, saldırı önleme ve müdahale konularında uzmanlaşmış ekiplerdir. Uluslararası düzeyde siber güvenliğin sağlanmasında kritik roller üstlenir.

Uluslararası iş birliği mekanizmaları, hukuki yardım, delil paylaşımı, şüphelilerin iadesi gibi alanlarda standart prosedürler geliştirerek bilişim suçlarıyla mücadeleyi güçlendirmektedir.

DÖRDÜNCÜ BÖLÜM

BİLİŞİM SUÇLARI İLE MÜCADELE VE ÖRNEK YARGI KARARLARI

4.1. Türkiye'de Bilişim Suçlarına İlişkin Yargı Kararlarının Genel Görünümü

Bilişim suçları, teknolojinin hızla gelişmesiyle birlikte hukuk sistemlerinde önemli bir yer tutmaya başlamış ve Türkiye'de de bu alanda yoğun yargı faaliyetleri gözlenmektedir. Türkiye'de bilişim suçlarına ilişkin yargı kararları, suçun türüne, işlendiği ortam ve yönteme bağlı olarak çeşitlilik göstermekte ve TCK ile 5651 sayılı Kanun gibi mevzuatlar çerçevesinde değerlendirilmektedir (Kara, 2019: 42).

Son yıllarda bilişim suçları alanında alınan kararlar, özellikle kişisel verilerin izinsiz kullanımı, bilişim sistemlerine yetkisiz erişim, bilişim yoluyla dolandırıcılık ve sahtecilik gibi suç tiplerinde yoğunlaşmıştır (Demir ve Yalçın, 2020: 110). Yargı kararları incelendiğinde, mahkemelerin suçun mağdur üzerindeki etkisini, suçun işleniş biçimini ve failin kastını detaylı değerlendirdiği görülmektedir (Öztürk, 2021: 75).

Türkiye'de bilişim suçlarıyla ilgili yargı kararlarının genel görünümünde dikkat çeken bir unsur, ceza yaptırımlarının caydırıcılık amacıyla artırılmasıdır. 5237 sayılı TCK'nın bilişim suçlarına ilişkin maddelerinde yapılan değişikliklerle, bu suçlara verilen cezaların ağırlığı artırılmış ve suçun niteliğine göre hapis ve para cezası gibi yaptırımlar öngörülmüştür (Aksoy, 2018: 88). Özellikle bilişim sistemlerine zarar verme ve kişisel verileri hukuka aykırı şekilde ele geçirme suçlarında mahkemeler, fail lehine herhangi bir indirime gitmeden ağır cezalara hükmetmektedir (Gündüz, 2020: 132).

Yargı kararlarında, bilişim suçlarının kanıtlanmasına yönelik teknik delillerin önemi de giderek artmaktadır. Bilirkişi raporları, dijital verilerin incelenmesi ve log kayıtları gibi teknik unsurlar, mahkemelerin kararlarında belirleyici olmaktadır (Şahin ve Demirtaş, 2022: 94). Bu bağlamda, adli bilişim alanındaki gelişmeler, bilişim suçlarıyla mücadelede etkinliğin artırılmasına önemli katkılar sağlamaktadır.

Türkiye’de bilişim suçlarına ilişkin yargı kararlarında yaşanan en önemli sorunlardan biri, suç tiplerinin hızla çeşitlenmesi ve teknolojinin sürekli gelişmesidir. Bu durum, mahkemelerin mevcut mevzuat kapsamında karar vermesini zorlaştırmakta ve hukuki boşlukların ortaya çıkmasına neden olmaktadır (Yılmaz, 2019: 56). Ayrıca, yargı mensuplarının bilişim teknolojileri alanında yeterli bilgi ve deneyime sahip olmaması da karar süreçlerinde güçlük yaratmaktadır (Özkan, 2021: 119).

Bununla birlikte, son dönemde yargı kararlarında bilişim suçlarına karşı daha bilinçli ve hızlı yaklaşımlar geliştiği görülmektedir. Özellikle büyükşehirlerdeki ağır ceza mahkemeleri, bilişim suçlarıyla ilgili dosyalarda uzmanlaşma eğilimindedir. Bu gelişme, suçun etkili şekilde tespiti ve faillerin cezalandırılması açısından olumlu bir adımdır (Kaya ve Arslan, 2022: 101).

Türkiye’de bilişim suçlarına ilişkin yargı kararlarında dikkat çeken diğer bir husus ise mağdur haklarının korunmasına verilen önemdir. Mahkemeler, özellikle kişisel verilerin izinsiz kullanılması veya yayımlanması halinde, mağdurun zararının giderilmesine yönelik tazminat taleplerini olumlu karşılamakta ve haksız fiil sorumluluğunu temel almaktadır (Demirtaş, 2020: 74). Ayrıca, kamuoyunun ve mağdurların bilişim suçlarına karşı bilinçlendirilmesi amacıyla mahkeme kararlarının şeffaflığına önem verilmektedir (Erdoğan, 2021: 59).

Özetle, Türkiye’de bilişim suçlarına ilişkin yargı kararları, teknolojik gelişmelerin ve yeni suç tiplerinin ortaya çıkmasının etkisiyle sürekli evrilmektedir. Mahkemeler, mevcut mevzuatı etkin kullanmaya çalışırken, bilişim suçlarının önlenmesi ve faillerin cezalandırılması konusunda önemli adımlar atmaktadır. Ancak, hukuki altyapının güçlendirilmesi, adli bilişim kapasitesinin artırılması ve yargı mensuplarının bilişim alanında eğitilmesi gibi konuların önümüzdeki dönemde öncelikli olması gerekmektedir (Çelik ve Yılmaz, 2021: 135).

4.2. E-Devlet ve Dijital Hizmetlerde Bilişim Suçlarına Dair Yargı Kararları

KARAR 1:

T.C.
Bölge Adliye Mahkemesi
Bursa 8. Ceza Dairesi
Esas No: 2021/2231
Karar No: 2023/1113
Karar Tarihi: 24-05-2023

Başkasına ait banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlam suçu – Yapılan alışverişlere ait işlemlerdeki IP numarası belirlenmiş ise de bu işlemlerdeki IP PORT numarasının tespiti ile suç zamanında kime ait olduğunun IP PORT numarası da verilerek tespiti sanığa mahkumiyet kararı verilmesinin düşünülmesi halinde malların iade edilmesi göz önünde bulundurularak eylemin teşebbüs aşamasında kalıp kalmadığının tartışılmasında zorunluluk bulunduğu – Hükmün bozulması

ÖZET: Sanık C. S.'in ilk derece mahkemesine vermiş olduğu beyanında; "IP internet kafeme aittir, şu an internet kafe kapalıdır" şeklinde beyanda bulunduğu, bunun üzerine ilk derece mahkemesince herhangi bir araştırma yapılmadan, sanığın beraatine karar verilmesinin hatalı olduğu, mahkemece kolluk kuvvetine müzekkere yazılarak söz konusu adreste suç tarihinde sanığın internet kafe işletip işletmediğinin tespiti, sanığa söz konusu yerin vergi kaydının olup olmadığının da sorularak vergi kaydının dosya içerisine konulmasının gerekliliği, Yapılan alışverişlere ait işlemlerdeki IP numarası belirlenmiş ise de bu işlemlerdeki IP PORT numarasının tespiti ile suç zamanında kime ait olduğunun IP Port numarası da verilerek tespiti, sanığa mahkumiyet kararı verilmesinin düşünülmesi halinde malların iade edilmesi göz önünde bulundurularak eylemin teşebbüs aşamasında kalıp kalmadığının tartışılmasında zorunluluk bulunduğu bozmayı gerektirmiştir.
(5271 S. K. m. 223) (5237 S. K. m. 53, 245)

İlk derece mahkemesince verilen hükme karşı Cumhuriyet Savcısı tarafından istinaf kanun yoluna başvurulmakla, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya incelenip görüşüldü;

İstinaf başvurusunun reddi nedenleri bulunmadığından işin esasına geçildi.

Tavşanlı Cumhuriyet Başsavcılığının 19/10/2020 tarih ve 2020/840 Esas sayılı iddianamesi ile sanık hakkında açılan kamu davasının yapılan yargılaması sonucunda Tavşanlı 1. Asliye Ceza Mahkemesi'nin 22/03/2021 tarih ve 2020/437 (E) ve 2021/253 (K) sayılı ilamıyla sanık hakkında CMK 223/2-e maddesi gereğince beraat kararı verildiği, verilen karara karşı Cumhuriyet Savcısı tarafından yasal süresi içerisinde istinaf kanun yoluna başvurduğu anlaşılmakla,

Cumhuriyet Savcısı istinaf dilekçesinde özetle; "Katılanın izni ve bilgisi dışında kullanmakta olduğu kredi kartından yapılan alışverişin .... IP numarasının kullanılarak yapıldığının tespit edildiği, sözkonusu IP numarasının suç tarihinde sanık C. S. adına kayıtla olduğu, Sanık C. S. alınan ifadesinde her ne kadar 2017 yılından beri İstanbul/Esenyurt'ta .....isimli bir kafe işlettiğini, kafe işletmecisi olduğu için WİFİ şifresini müşterileriyle paylaştığını beyan etmişse de suçtan kurtulmaya yönelik beyanlarına itibar edilmediği, sanığın üzerine atılı suçu işlediği anlaşılmakla; sanığın 5237 Sayılı TCK nun 245/1 ve 53 maddeleri uyarınca cezalandırılması gerekirken sanığa isnat edilen eylemlerin sanık tarafından işlendiğinin sabit olmadığı gerekçesiyle beraat kararı verilmesi nedeniyle, usul ve esas yönünden Kanun'a aykırı bulunduğundan kararın istinâfen kaldırılması arz olunur." şeklinde istinaf talebinde bulunduğu,

Dosya incelendi.

Sanık C. S.'in ilk derece mahkemesine vermiş olduğu beyanında; "IP internet kafeme aittir, şu an internet kafe kapalıdır" şeklinde beyanda bulunduğu, bunun üzerine ilk derece mahkemesince herhangi bir araştırma yapılmadan, sanığın beraatine karar verilmesinin hatalı olduğu, mahkemece kolluk kuvvetine müzekkere yazılarak söz konusu adreste suç tarihinde sanığın internet kafe işletip işletmediğinin tespiti, sanığa söz konusu yerin vergi kaydının olup olmadığının da sorularak vergi kaydının dosya içerisine konulmasının gerekliliği,
Yapılan alışverişlere ait işlemlerdeki IP numarası belirlenmiş ise de bu işlemlerdeki IP PORT numarasının tespiti ile suç zamanında kime ait olduğunun IP Port numarası da verilerek tespiti, sanığa mahkumiyet kararı verilmesinin düşünülmesi halinde malların iade edilmesi göz önünde bulundurularak eylemin teşebbüs aşamasında kalıp kalmadığının tartışılmasında zorunluluk bulunduğu,

Bozmayı gerektirmiş, Cumhuriyet Savcısı'nın talepleri bu itibarla yerinde görülmüş olduğundan 5271 sayılı CMK 289/1 maddesi uyarınca ilk derece mahkemesi kararının BOZULMASINA,

Dosyanın, yeniden incelenmek ve hükmolunmak üzere hükmü veren ilk derece mahkemesine GÖNDERİLMESİNE,

Dair, dosya üzerinde yapılan inceleme sonucunda 5271 sayılı CMK'nın 284. ve 286. maddeleri gereğince KESİN olmak üzere 24/05/2023 tarihinde oybirliğiyle karar verildi.

Kararda, malların iade edilmesi göz önünde bulundurularak eylemin teşebbüs aşamasında kalıp kalmadığının tartışılmasında zorunluluk bulunduğundan hükmün bozulmasına karar verilmiştir.

KARAR 2:

T.C.
Bölge Adliye Mahkemesi
Antalya 9. Ceza Dairesi
Esas No: 2022/4012
Karar No: 2023/1744
Karar Tarihi: 12-05-2023

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Banka veya kredi kartlarının kötüye kullanılması suçu – Kartların farklı zamanlarda kopyalanıp üretildiğine ilişkin delil bulunmaması – Zincirleme suç hükümleri uygulanması suretiyle fazla ceza tayin edilmesi – Hükmün düzeltilerek istinaf başvurularının ayrı ayrı esastan reddi

ÖZET: Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede; Sanıkların üzerilerine atılı Başkalarına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Banka veya Kredi Kartı Üretme,Satma vb., Yasak Cihaz ve Program Bulundurmak suçlarından mahkumiyetlerine dair mahkemenin kabul ve uygulamasında eleştirilen hususlar dışında usul ve yasaya aykırılık bulunmadığı, ancak; mağdur … Bankası A.Ş' ne yönelik kartların farklı zamanlarda kopyalanıp üretildiğine ilişkin delil bulunmaması nedeniyle sanıkların TCK'nın 245/2 maddesinden bir kez cezalandırılması yerine zincirleme suç hükümleri uygulanması suretiyle fazla ceza tayin edilmesi hatalı olduğu, bu yanılgının davanın yeniden görülmesini ve olayın daha fazla aydınlatılmasını gerektirmediği ve düzeltilebilir nitelikte olduğu anlaşılmakla hükmün düzeltilerek istinaf başvurularının ayrı ayrı esastan reddine karar verilmiştir.
(5237 S. K. m. 62, 245, 245/A)

Yerel Mahkemece verilen hükümlere karşı istinaf yoluna başvurulmakla, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya görüşüldü:

İstinaf başvurusunun reddi nedenleri bulunmadığından işin esasına geçildi. Bir kısım sanıkların gözaltında ve tutuklulukta kaldığı sürelerin gerekçeli karar başlığında gösterilmemesi hatalı ise de; bu husus mahallinde düzeltilebilir hata olarak değerlendirilmiştir.

Sanık E. Ş. A. hakkında kurulan hükümlerde soyadının yanlış yazılması hatalı ise de; bu husus mahallinde düzeltilebilir maddi hata olarak değerlendirilmiştir.

Sanıklar E. Ş. A. ve B. Ö. haklarında TCK'nın 245/2 Maddesinden kurulan hükümlerde aynı yasanın 62. Maddesinin uygulanmamasında bir isabetsizlik bulunmadığı ancak; 245/A Maddesinde kurulan hükümlerde yasanın amacına aykırı olacak şekilde TCK'nın 62/1. Maddesinin uygulanması suretiyle eksik ceza tayini hatalı ise de; aleyhe istinaf bulunmadığından bu husus eleştirilmekle yetinilmiştir.

Sanık T. B. N.' ın Aydın 2. Asliye Ceza Mahkemesinin 24/03/2015 gün, 2014/529 Esas ve 2015/192 Karar sayılı ilamı nedeni ile 2. kez mükerrir olduğu halde, mahkemece Trabzon 3. Asliye Ceza Mahkemesinin 2016/176 esas 2016/470 karar sayılı ilamının tekerrüre esas alınarak birinci kez tekerrür hükümlerinin uygulanmış olması hatalı ise de; aleyhe istinaf bulunmadığından bu husus eleştirilmekle yetinilmiştir.

Tekerrür hükümleri uygulanan sanık T. B. N. hakkında TCK'nın 62. Maddesinin uygulanması hatalı ise de, aleyhe istinaf bulunmadığından bu husus eleştirilmekle yetinilmiştir.

Tekerrür hükümleri uygulanan sanık B. Ö. hakkında TCK'nın 245/A Maddesinden hüküm kurulurken TCK'nın 62. Maddesinin uygulanması hatalı ise de; aleyhe istinaf bulunmadığından bu husus eleştirilmekle yetinilmiştir.

Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede; Sanıkların üzerlerine atılı Başkalarına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Banka veya Kredi Kartı Üretme, Satma vb., Yasak Cihaz ve Program Bulundurmak suçlarından mahkumiyetlerine dair mahkemenin kabul ve uygulamasında eleştirilen hususlar dışında usul ve yasaya aykırılık bulunmadığı,

Ancak;

Yargıtay 8. Ceza Dairesinin 2021/16672 Esas 2022/6003 Karar sayılı benzer ilamında da belirtildiği üzere söz konusu mağdur Türk Ekonomi Bankası A.Ş' ne yönelik kartların farklı zamanlarda kopyalanıp üretildiğine ilişkin delil bulunmaması nedeniyle sanıkların TCK'nın 245/2 maddesinden bir kez cezalandırılması yerine zincirleme suç hükümleri uygulanması suretiyle fazla ceza tayin edilmesi hatalı olduğu, bu yanılgının davanın yeniden görülmesini ve olayın daha fazla aydınlatılmasını gerektirmediği ve düzeltilebilir nitelikte olduğu anlaşılmakla;

Sanıklar hakkında 245/2. Maddesinden kurulan mahkumiyet hükümlerinde yer alan TCK'nın 43/1. Maddesinin uygulandığı bölümlerin tamamen HÜKÜMDEN ÇIKARTILMASINA,

Sanıklar E. Ş. N., B. Ö.' in 3 YIL HAPİS VE 5 GÜN KARŞILIĞI ADLİ PARA CEZASI İLE CEZALANDIRILMALARINA,

Bu sanıklar yönünden hükmün Adli Para Cezasının belirlendiği bentlerde geçen "120 TL " ibarelerinin hükümden çıkartılarak yerine (5 X 20= 100) "100 TL" ibarelerinin yazılmasına,

Sanıklar Ö. T., Y. K., M. B., T. B. N. yönünden 62/1. Maddesinin uygulandığı bölümde yer alan "3 YIL 1 AY 15 GÜN HAPİS VE 5 GÜN KARŞILIĞI ADLİ PARA CEZASI İLE CEZALANDIRILMASINA " ibarelerinin hükümden çıkartılarak yerlerine "2 YIL 6 AY HAPİS VE 4 GÜN " ibaresinin yazılmasına,

Bu sanıklar yönünden hükmün Adli Para Cezasının belirlendiği bentlerde geçen "100 TL " ibarelerinin hükümden çıkartılarak yerine (4 X 20= 80) "80 TL" olarak yazılmasına ve hükümde yer alan diğer hususların aynen muhafazası suretiyle 5271 Sayılı CMK'nın 7035 Sayılı Yasanın 15. Maddesi ile Değişik 280/1-a ve 303/1-a Maddeleri uyarınca HÜKMÜN DÜZELTİLEREK İSTİNAF BAŞVURULARININ AYRI AYRI ESASTAN REDDİNE,

Dosyanın hükmü veren ilk derece mahkemesine gönderilmesine CMK'nın 286/2-a Maddesi gereğince KESİN olarak 12/05/2023 tarihinde oybirliğiyle karar verildi.

Kararda TCK'nın 245/2 maddesinden bir kez cezalandırılması yerine zincirleme suç hükümleri uygulanması suretiyle fazla ceza tayin edilmesi hatalı olduğu, bu yanılgının davanın yeniden görülmesini ve olayın daha fazla aydınlatılmasını gerektirmediği ve düzeltilebilir nitelikte olduğu anlaşılmakla hükmün düzeltilerek istinaf başvurularının ayrı ayrı esastan reddine karar verilmiştir.

KARAR 3:

Bölge Adliye Mahkemesi
Trabzon 3. Ceza Dairesi
Esas No: 2023/804
Karar No: 2023/831
Karar Tarihi: 17-05-2023

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Dolandırıcılık suçu – Söz konusu GSM hattının sadece dolandırıcılık eylemlerinde kullanılmak üzere çıkartılan patates hat diye tabir edilen hatlardan olduğunun anlaşıldığı – Yine bu hesaptan aktarım yapılan ENPARA hesabının da kendisine ait olduğunu – Görevsizlik kararının kaldırılması

ÖZET: Müştekinin şikayete konu olay ile ilgili görüşme sağladığı 0554 ... nolu gsm hattının yabancı uyruklu D. R. adına kayıtlı olduğu, söz konusu gsm hattının sadece dolandırıcılık eylemlerinde kullanılmak üzere çıkartılan "patates hat" diye tabir edilen hatlardan olduğunun anlaşıldığı, bu sebeplerle D. R. hakkında üzerine atılı kişinin, kendisini kamu görevlisi veya

banka, sigorta, kredi kurumlarının çalışanı olarak tanıtması veya bu kurumlarla ilişkili olduğunu söylemesi suretiyle dolandırıcılık suçunu işlediğine dair kamu davası açmaya yeterli şüpheye ulaşılamadığından hakkında ek takipsizlik kararı verildiği, Müştekinin para yatırmış olduğu banka hesabının sahibi olan şüpheli E. T. A., olayla ilgili 24/05/2022 tarihli savunmasında özetle, suça konu banka hesabının kendisine ait olduğunu, yine bu hesaptan aktarım yapılan enpara hesabının da kendisine ait olduğunu, hesabının kullanması için başkaca bir şahsa vermediğini ve ancak hesabını yaklaşık 7-8 aydır kullanmadığını üzerine atılı suçlamaları kabul etmediğini beyan ettiği, Para çekim anına ait görüntüler ile şüpheli E. T. A.'ın görüntüleri arasında yapılan inceleme sonrası hazırlanan Ankara Bölge Kriminal Polis Laboratuvarı Müdürlüğü'nün 07/10/2022 tarihli uzmanlık raporunda görüntülerdeki şahsın şüpheli E. T. A. ile muhtemel farklı kişiler olduğunun tespit edilmiştir.

(5237 S. K. m. 142, 245) (5271 S. K. m. 225, 280, 289)

Sanıklar hakkında yapılan yargılama sırasında; Trabzon 6. Asliye Ceza Mahkemesiyle Trabzon 3. Ağır Ceza Mahkemesi arasında oluşan olumsuz görev uyuşmazlığının giderilmesi ve yargı yerinin belirlenmesi istemiyle gönderilen dosya incelendi.

GEREĞİ DÜŞÜNÜLDÜ:

Sanık hakkında Trabzon Cumhuriyet Başsavcılığı'nın 08.02.2023 tarih ve 2023/146 esas sayılı iddianamesi ile: "Müşteki A. F. A., 09/06/2021 tarihinde Çağlayan Jandarma Karakol Komutanlığı'na müracaat ederek 08/06/2021 günü saat 15:30 sıralarında 0554 ... nolu gsm hattından arayan kişinin kendisine, bankalar birliğinden aradığını ve daha önce kullanmış olduğu kredilerin masraflarının kendisine iade edileceğini bunun için banka ve kredi kartı bilgilerini kendisine vermesini istediğini, arayan şahsın kendisine ait T.C kimlik numarasını doğru okumasından dolayı güvendiğini ve bilgileri şahsa verdiğini sonrasında cep telefonuna gelen doğrulama şifrelerini de şahsa verdiğini ve konuştuğu kişinin paraların kendisine peyder pey yatacağını söyleyerek telefonu kapattığını, aynı gün saat 17:05, 17:09, 17:23, 17:24, 17:26, 17:27'de olmak üzere 6 farklı mesajda her seferinde 1.000 TL olmak üzere hesabından toplamda 6.000 TL çekildiğine dair mesaj geldiğini ve bunun üzerine dolandırıldığını anladığını ve hesaplarını iptal ettirdiğini kendisini bu şekilde dolandıran şahıs veya şahıslardan davacı ve şikayetçi olduğunu beyan etmesi üzerine olayla ilgili Cumhuriyet Başsavcılığımızca soruşturmaya başlanılmış ise de,

Müştekinin şikayete konu olay ile ilgili görüşme sağladığı 0554 ... nolu gsm hattının yabancı uyruklu D. R. adına kayıtlı olduğu, söz konusu gsm hattının sadece dolandırıcılık eylemlerinde kullanılmak üzere çıkartılan "patates hat" diye tabir edilen hatlardan olduğunun anlaşıldığı, bu sebeplerle D. R. hakkında üzerine atılı kişinin, kendisini kamu görevlisi veya banka, sigorta, kredi kurumlarının çalışanı olarak tanıtması veya bu kurumlarla ilişkili olduğunu söylemesi suretiyle dolandırıcılık suçunu işlediğine dair kamu davası açmaya yeterli şüpheye ulaşılamadığından hakkında ek takipsizlik kararı verildiği,

Müştekinin para yatırmış olduğu banka hesabının sahibi olan şüpheli E. T. A., olayla ilgili 24/05/2022 tarihli savunmasında özetle, suça konu banka hesabının kendisine ait olduğunu, yine bu hesaptan aktarım yapılan enpara hesabının da kendisine ait olduğunu, hesabının kullanması için başkaca bir şahsa vermediğini ve ancak hesabını yaklaşık 7-8 aydır kullanmadığını üzerine atılı suçlamaları kabul etmediğini beyan ettiği,

Para çekim anına ait görüntüler ile şüpheli E. T. A.'ın görüntüleri arasında yapılan inceleme sonrası hazırlanan Ankara Bölge Kriminal Polis Laboratuvarı Müdürlüğü'nün 07/10/2022 tarihli uzmanlık raporunda görüntülerdeki şahsın şüpheli E. T. A. ile muhtemel farklı kişiler olduğunun tespit edildiği,

Tüm bilgi belge ve beyanlar birlikte değerlendirildiğinde,

Her ne kadar şüpheli üzerine atılı suçlamaları kabul etmediğini beyan etse de, şüphelinin hesabına yatan banka kartını başkaca bir şahsa kullanması için vermediğini beyan etmesi, müştekinin hesabından şüphelinin hesabına aktarılan paranın yine şüpheliye ait en para hesabına paranın havale edilmiş olması, şüphelinin savunması göz önüne alındığında suç tarihinde şüphelinin söz konusu banka hesabını aktif olarak kullanıyor olduğunun anlaşılması ve şüphelinin banka hesap hareketleri incelendiğinde başkaca şahıslar tarafından da şüphelinin hesabına para transferleri yapıldığının görülmesi ve şüpheli hakkında ülke genelinde benzer şekildeki iddialarla soruşturma ve kovuşturma dosyasının bulunması hususları birlikte değerlendirildiğinde şüphelinin suçtan kurtulmaya yönelik hayatın olağan akışına aykırı beyanlarına itibar edilmediği,

Şüpheli E. T. A.'ın müşteki A. F. A.'ı hileli davranışlarıyla aldatıp müştekiyi 6.000 TL zarara uğratmak suretiyle üzerlerine atılı kişinin, kendisini kamu görevlisi veya banka, sigorta, kredi kurumlarının çalışanı olarak tanıtması veya bu kurumlarla ilişkili olduğunu söylemesi suretiyle dolandırıcılık suçunu işlediklerine dair kamu davası açmaya yeterli şüpheye ulaşıldığından, şüphelinin cezalandırılması istemiyle mahkememize kamu davası açılmış ise de;

İddianamede; "...Müşteki A. F. A., 09/06/2021 tarihinde Çağlayan Jandarma Karakol Komutanlığı'na müracaat ederek 08/06/2021 günü saat 15:30 sıralarında 0554 ...nolu gsm hattından arayan kişinin kendisine, bankalar birliğinden aradığını ve daha önce kullanmış olduğu kredilerin masraflarının kendisine iade edileceğini bunun için banka ve kredi kartı bilgilerini kendisine vermesini istediğini, arayan şahsın kendisine ait T.C kimlik numarasını doğru okumasından dolayı güvendiğini ve bilgileri şahsa verdiğini sonrasında cep telefonuna gelen doğrulama şifrelerini de şahsa verdiğini ve konuştuğu kişinin paraların kendisine peyder pey yatacağını söyleyerek telefonu kapattığını, aynı gün saat 17:05, 17:09, 17:23, 17:24, 17:26, 17:27'de olmak üzere 6 farklı mesajda her seferinde 1.000 TL olmak üzere hesabından toplamda 6.000 TL çekildiğine dair mesaj geldiğini şahsın kendisine ait T.C kimlik numarasını doğru okumasından dolayı güvendiğini ve bilgileri şahsa verdiğini sonrasında cep telefonuna gelen doğrulama şifrelerini de şahsa verdiğini ve konuştuğu kişinin paraların kendisine peyder pey yatacağını söyleyerek telefonu kapattığını, aynı gün saat 17:05, 17:09, 17:23, 17:24, 17:26, 17:27'de olmak üzere 6 farklı mesajda her seferinde 1.000 TL olmak üzere hesabından toplamda 6.000 TL çekildiğine dair mesaj geldiğini ve bunun üzerine dolandırıldığını anladığını..."; dolayısıyla, hileli hareketlerle veya başka bir yolla müştekinin banka hesabına ilişkin bilgilerinin ele geçirilerek, banka hesabından bilgi ve rızası dışında başka bir hesaba/hesaplara havale yapılmak veya para çekilmesi suretiyle menfaat temin edildiği iddia edilen olayda; sübutu halinde sanığın eyleminin "Nitelikli Dolandırıcılık" suçunu değil, Asliye Ceza Mahkemesinin görev alanındaki TCK'nın 142/2-e maddesinde yazılı "Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık" suçunun veya koşullarının oluşması halinde yine Asliye Ceza Mahkemesinin görev alanındaki TCK'nın 245/1. Maddesindeki yazılı suçu oluşturacağı, dolayısıyla sanığa yüklenen suça bakma görevinin Asliye Ceza Mahkemesine ait olduğu belirtilerek görevsizlik kararı verilmiştir.

Trabzon 6. Asliye Ceza Mahkemesinde yapılan değerlendirmede;

Her ne kadar sanık hakkında kişinin, kendisini kamu görevlisi veya banka, sigorta, kredi kurumlarının çalışanı olarak tanıtması veya bu kurumlarla ilişkili olduğunu söylemesi suretiyle dolandırıcılık suçundan görevsizlik kararı verilerek dosya mahkememize gönderilmiş ise de; dosya kapsamı incelendiğinde, eylemin TCK 158/1-L madde ve fıkrasında belirtilen kişinin kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delillerin takdirinin üst dereceli ağır ceza mahkemesine ait olduğu gözetilerek eylemin nitelikli dolandırıcılık suçunu oluşturması ihtimali ile delilleri tartışma ve CMK 3-4-5 gereği öngörülen suça ilişkin yargılama görevinin Ağır Ceza Mahkemelerine ait olduğu belirtilip karşı görevsizlik kararı verilmiştir.

CMK'nın 225 maddesi gereğince hükmün konusunu oluşturacak iddianamede sanığın kendisini bankalar birliği çalışanı olarak tanıtmak suretiyle mağduru dolandırdığı iddia edilmektedir.

Yargıtay İçtihatlarında sanığın kendisini banka veya kamu çalışanı tanıtması halinde eylemin Ağır Ceza Mahkemesince değerlendirmesi gerektiği belirtilmektedir.

"...Benzer bir olaya ilişkin Yargıtay 15. Ceza Dairesinin 21/12/2020 tarihli ve 2019/14189 esas 2020/12683 karar sayılı ilamında yer alan '...Sanıkların kendilerini kamu görevlisi, banka ve kredi kurumunun çalışanı olarak tanıttıklarının iddia edilmesi karşısında sanıklara isnat edilen eylemin 5237 sayılı TCK'nın 158/1-L maddesinde öngörülen nitelikli dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delillerin takdirinin üst dereceli Ağır Ceza Mahkemesine ait olduğu gözetilerek görevsizlik kararı verilmesinde zorunluluk bulunması, arayan şahsın kendisini banka görevlisi olarak tanıtması ve müştekinin de bu hususa inanarak istenilen bilgileri vermesi karşısında sanıklara yüklenen eylemlerin 5237 Sayılı Kanunun 158/1-L maddesinde düzenlenen Nitelikli Dolandırıcılık suçunu oluşturup oluşturmadığına ilişkin delillerin değerlendirilmesinin üst dereceli mahkemeye ait olduğu

gözetilmeden itirazın reddi yerine yazılı şekilde kabulüne karar verilmesinde isabet görülmediğinden..." (Y11CD 2021/41595 E, 2022/1402 K. 27/01/2022)

Yukarıda belirtilen nedenler ve Yargıtay İçtihatı göz önüne alınarak iddianamede anlatılan eyleme ilişkin yargılama yapma görev ve yetkisi Ağır Ceza Mahkemesine ait olduğu değerlendirilmekle Trabzon 3. Ağır Ceza Mahkemesinin görevsizlik kararının kaldırılmasına karar vermek gerekmiş ve aşağıdaki şekilde hüküm kurulmuştur.

HÜKÜM: Yukarıda belirlenen gerekçelerle;

Yukarıda belirtilen gerekçe ve Yargıtay İçtihatı göz önüne alınarak Trabzon 3. Ağır Ceza Mahkemesinin 24/02/2023 tarih, 2023/148 Esas, 2023/58 Karar sayılı görevsizlik kararının kaldırılmasına,

Dosyanın gereğinin takdir ve ifası için mahalline iadesine,

5271 sayılı CMK'nın 4 ve 286 maddeleri uyarınca KESİN olmak üzere 17/05//2023 tarihinde oybirliği ile karar verildi.

Kararda söz konusu TCK M. 245/1 yazılı suçu oluşturacağı ve GSM hattının sadece dolandırıcılık eylemlerinde kullanmak üzere çıkartılan patates hat diye tabir edilen hatlardan olduğunun anlaşıldığı yine bu hesaptan aktarım yapılan enpara hesabının da kendisine ait olduğunu ve görevsizlik kararının kaldırılmasına karar verilmiştir.

KARAR 4:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2016/10781
Karar No: 2017/4966
Karar Tarihi: 03-05-2017

Bilişim suçu – Sanığın suçu kabul etmemesi – Sanığın şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği – Sanık eğer sadece şikayetçinin hesabına giriş yaptı ise bilişim sistemine izinsiz girme suçunun oluşacağının kabulü gereği.

ÖZET: Sanığın suçu kabul etmemesi, şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde e-mail şifresinin değiştirilmesine dair bir tespitin bulunmaması karşısında, kalmaya devam ettirdiğine ve şifre değiştirdiğine ilişkin deliller tespit edilip sonucuna göre hukuki durumunun takdir ve tayini, sanığın sadece giriş yaptığı ve kalmaya devam ettiğinin tespiti halinde ise eyleminin bilişim sistemine izinsiz girme suçunu oluşturacağının gözetilmesi gerekir.
(5237 S. K. m. 243)

Bilişim suçundan sanık ... hakkında 31.05.2011 tarihli verilen hükmün açıklanmasının geri bırakılmasına ilişkin karar kaldırılarak hükmün açıklanmasına ve 5237 sayılı TCK.nun 244/2. madde ve fıkrası uyarınca hükümlülüğüne dair; Kuşadası 1. Asliye Ceza Mahkemesinin 06.01.2015 gün ve 2014/478 esas, 2015/16 karar sayılı hükmün süresi içinde Yargıtay'ca incelenmesi sanık tarafından istenilmiş olduğundan dava evrakı Cumhuriyet Başsavcılığından tebliğname ile daireye gönderilmekle incelendi:

Gereği görüşülüp düşünüldü:

Şikayetçinin rızası olmadan e-mail ve Facebook hesabına girip şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; suç tarihi itibariyle yürürlükte olan TCK.nun 243/1. maddesinde "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden…" ibaresinin yer aldığı dikkate alınarak, sanığın suçu kabul etmemesi, şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde e-mail şifresinin değiştirilmesine dair bir tespitin bulunmaması karşısında, kalmaya devam ettirdiğine ve şifre değiştirdiğine ilişkin deliller tespit edilip sonucuna göre hukuki durumunun takdir ve tayini, sanığın sadece giriş yaptığı ve kalmaya devam ettiğinin tespiti halinde ise eyleminin TCK.nun 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,

Yasaya aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321. maddesi gereğince BOZULMASINA, 03.05.2017 gününde oybirliği ile karar verildi.

Kararda TCK m. 243/1 gereğince şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde e-mail şifresinin değiştirilmesine dair bir tespitin bulunmaması karşısında, kalmaya devam ettirdiğine ve şifre değiştirdiğine ilişkin deliller tespit edilip sonucuna göre hukuki durumunun takdir ve tayini, sanığın sadece giriş yaptığı ve kalmaya devam ettiğinin tespiti halinde ise eyleminin bilişim sistemine izinsiz girme suçunu oluşturacağının gözetilmesi gerektiğinden yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 5:

T.C.
YARGITAY
8. Ceza Dairesi
Esas No: 2017/897
Karar No: 2017/6019
Karar Tarihi: 25-05-2017

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine hukuka aykırı olarak girme suçu – Sanığın suçu kabul etmemesi ve dosya kapsamı – İlgili mail adresinin bilgilerinin bağlı olduğu şirketten suç tarihinde kimin kullanımında olduğunun araştırılması gereği

ÖZET: Sanığın suçu kabul etmemesi ve dosya kapsamına göre ilgili mail adresinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemi sistemi engelleme bozma verileri yok etme veya değiştirme suçunu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekir.

(5237 S. K. m. 243, 244)

Gereği görüşülüp düşünüldü:

Şikayetçi ...'ın 01.11.2011 tarihinde internette ... isimli oyunu oynarken ....com.tr adresinden arkadaşlık teklifi geldiğini, bu teklifi kabul ederek karşıdaki şahısla bu adresten konuştuğunu, tekrar oyuna döndüğünde oyun şifresinin çalınıp oyun karakterlerinin aldığından bahisle açılan davada, sanığın suçlamayı kabul etmemesi, anılan mail adresini kullanmadığını savunması, adli bilişim büro amirliğinin 17.07.2013 tarihli imaj alma tutanağında, sanığın evinde mikro-2 GB SD kart üzerinde yapılan incelemede suç unsuruna rastlanılmadığının bildirilmesi, bilirkişi tarafından düzenlenen 01.04.2014 tarihli raporda, oyun şifresini çalacak kadar bilgi ve beceriye sahip bir kişinin işlemi yapmış olduğu, bilgisayarın kullandığı IP adresinin de sisteme düşeceğini bileceği değerlendirildiğinden suçu işlediği hususunda kanaat oluşmadığının belirtilmesi, microsoft şirketinden gelen cevapta ....com.tr adresine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde araştırılmaması karşısında, anılan mail adresinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/4.

maddesindeki suçu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,

Yasaya aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321. ve 326/son maddeleri gereğince BOZULMASINA, 25.05.2017 gününde oybirliği ile karar verildi.

Kararda TCK m.243, 244 gereğince suç tarihinde mail adresinin kimin kullanımında olduğunun belirlenmesi, oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemi sistemi engelleme bozma verileri yok etme veya değiştirme suçunu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerektiğinden yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 6:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2017/1091
Karar No: 2017/12836
Karar Tarihi: 16-11-2017

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçu – Deneme süresi içinde suç işlendiğinden bahisle hükmün açıklanmasının talep – Duruşma açılarak taraflara usulen çağrı kağıdı çıkarılıp koşulların değerlendirilmesi gereği

ÖZET: Hükmün açıklanmasının geri bırakılması kararının kesinleşmesinden sonra, deneme süresi içerisinde suç işlendiğinden bahisle hükmün açıklanmasının talep olunması üzerine duruşma açılarak taraflara usulen çağrı kağıdı çıkarılıp, hükmün açıklanmasını gerektiren koşulların oluşup oluşmadığının değerlendirilmesi gerektiği gözetilmeden, yazılı şekilde evrak üzerinden ve duruşma açılmadan karar verilmesi yasaya aykırı olup kanuna yararına bozma talebinin kabulüyle hükmün bozulması gerekir.
(5237 S. K. m. 243) (5271 S. K. m. 231)

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan sanık ...'ın, 5237 sayılı Türk Ceza Kanunu'nun 243/1, 62 ve 52. maddeleri uyarınca 1.500,00 Türk Lirası adli para cezası ile cezalandırılmasına, 5271 sayılı Ceza Muhakemesi Kanunu'nun 231/5. maddesi gereğince sanık hakkındaki hükmün açıklanmasının geri bırakılmasına dair Çanakkale 2. Sulh Ceza Mahkemesinin 07/03/2012 tarihli ve 2011/654 esas, 2012/193 sayılı kararının kesinleşmesini müteakip, sanığın deneme süresi içerisinde yeniden suç işlediğinden bahisle 5271 sayılı Kanun'un 231/11. maddesi uyarınca sanık hakkında verilen hükmün açıklanmasına, 5237 sayılı Türk Ceza Kanunu'nun 243/1, 62 ve 52. maddeleri uyarınca 1.500,00 Türk Lirası adli para cezası ile cezalandırılmasına ilişkin Çanakkale 5. Asliye Ceza Mahkemesinin 26/07/2016 tarihli ve 2016/422 esas, 2016/733 sayılı kararını kapsayan dosya incelendi.

Benzer bir olay sebebiyle Yargıtay 2. Ceza Dairesinin 19/09/2008 tarihli ve 2008/12198 esas, 2008/9890 sayılı ilamında da belirtildiği üzere, 5271 sayılı Ceza Muhakemesi Kanunu'nun 231/11. fıkrasında yer alan "Denetim süresi içinde kasten yeni bir suç işlemesi veya denetimli serbestlik tedbirine ilişkin yükümlülüklere aykırı davranması halinde, mahkeme hükmü açıklar. Ancak mahkeme, kendisine yüklenen yükümlülükleri yerine getiremeyen sanığın durumunu değerlendirerek; cezanın yarısına kadar belirleyeceği bir

kısmının infaz edilmemesine ya da koşullarının varlığı halinde hükümdeki hapis cezasının ertelenmesine veya seçenek yaptırımlara çevrilmesine karar vererek yeni bir mahkûmiyet hükmü kurabilir." şeklindeki düzenleme nazara alındığında, mahkemece duruşma açılmasını müteakip, sanığın celp edilmesi, varsa diyecekleri sorulup, anılan fıkra uyarınca değerlendirme yapıldıktan sonra hüküm kurulması gerektiği gözetilmeden, dosya üzerinden karar verilmesinde isabet görülmediğinden bahisle 5271 sayılı CMK.nun 309. maddesi uyarınca anılan kararın bozulması lüzumu Yüksek Adalet Bakanlığı Ceza İşleri Genel Müdürlüğünün 20/12/2016 gün ve 11407 sayılı kanun yararına bozma istemine atfen Yargıtay C. Başsavcılığının 11/01/2014 gün ve KYB/2016-402288 sayılı ihbarnamesi ile dairemize tevdii kılınmakla incelendi.

TÜRK MİLLETİ ADINA

Gereği görüşülüp düşünüldü:

Hükmün açıklanmasının geri bırakılması kararının kesinleşmesinden sonra, deneme süresi içerisinde suç işlendiğinden bahisle hükmün açıklanmasının talep olunması üzerine duruşma açılarak taraflara usulen çağrı kağıdı çıkarılıp, hükmün açıklanmasını gerektiren koşulların oluşup oluşmadığının değerlendirilmesi gerektiği gözetilmeden, CMK.nun 231/11. madde ve fıkrasına aykırı olarak yazılı şekilde evrak üzerinden ve duruşma açılmadan karar verilmesi, Yasaya aykırı ve Adalet Bakanlığı'nın Kanun Yararına Bozma istemine dayalı Yargıtay Cumhuriyet Başsavcılığının ihbarname içeriği bu itibarla yerinde görüldüğünden Çanakkale 5. Asliye Ceza Mahkemesinin 26.7.2016 gün, 2016/422 esas, 2016/733 sayılı kararının CMK.nun 309. maddesi gereğince BOZULMASINA, müteakip işlemlerin mahallinde yapılmasına, dosyanın Adalet Bakanlığına gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına tevdiine, 16.11.2017 gününde oybirliği ile karar verildi.

Kararda, TCK m. 243 gereğince duruşma yapılmadan dosya üzerinden karar verilmesi yasaya aykırı olduğundan yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 7:

T.C.
YARGITAY
11.Ceza Dairesi
Esas No: 2017/3943
Karar No: 2019/6476
Karar Tarihi: 19-09-2019

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Kamu görevlisinin resmi belgede sahteciliği suçu – Memurun resmi belgede sahteciliği suçuna azmettirme suretiyle iştirak suçunu oluşturacağı gözetilmeden yardım eden sıfatıyla cezalandırılması suretiyle eksik ceza tayini – Hükmün bozulması

ÖZET: TCK'nin ... maddesine göre, özgü suçlarda özel faillik niteliği taşıyan kişilerin fail olabileceği bu suçun işlenişine iştirak eden diğer kişilerin ise ancak azmettiren veya yardım eden olarak sorumlu tutulabileceği cihetle, sanık ...'un eyleminin TCK'nin … maddeleri delaletiyle "memurun resmi belgede sahteciliği suçuna azmettirme suretiyle iştirak" suçunu oluşturacağı gözetilmeden, yardım eden sıfatıyla cezalandırılması suretiyle eksik ceza tayini, bozmayı gerektirmiştir.
(5237 S. K. m. 38, 40, 244)

1-Olay tarihinde meydana gelen kasten öldürme suçunun firari şüphelisi olan ve hakkında yakalama kararı bulunan sanık ...'un avukatı aracılığı ile Şanlıurfa Cumhuriyet Başsavcılığına 05.01.2011 tarihinde ... Devlet Hastanesi'nde tedavi gördüğüne dair belge ibraz ettiği, belgenin doğruluğunun teyidi amacıyla yapılan yazışmalar sonucunda ibraz edilen belgenin sahte olduğunun anlaşılması, sanık ...'in girişini otomasyon görevlisi olan sanıklardan sanık ...'nin, tanı girişini ise sanık ...'nin yaptığı iddiasıyla kamu görevlisinin resmi belgede sahteciliği suçundan açılan kamu davasının yargılaması sonucunda, her ne kadar sanıkların mahkumiyetine karar verilmiş ise de; yapılan incelemede, 25.01.2011 tarihli belgeye

05.01.2011 tarihli barkod yapıştırılmak suretiyle oluşturulan suça konu sahte belgenin sanık ...'in avukatı tarafından dosyaya fotokopisinin ibraz edildiği ve tüm dosya kapsamından suça konu belgenin aslının ele geçirilemediğinin anlaşılması karşısında; Yargıtay Ceza Genel Kurulunun 14.10.2003 gün ve 232-250 sayılı, 09.10.2012 gün ve 2011/8-335 Esas 2012/1804 sayılı kararlarında da açıklandığı üzere, fotokopi belgenin hukuki sonuç doğurmaya elverişli nitelikte olmayacağı ve aslı bulunmayan belgenin aldatma niteliği tespit edilemeyeceğinden resmi belgede sahtecilik suçunun unsurları itibariyle oluşmadığı, ancak; somut olayda hastane bilgisayar sistemine girilerek 05.01.2011 tarih ve... nolu barkodun oluşturularak aslı ele geçirilemeyen suça konu belgeye yapıştırıldığının anlaşılması karşısında, sanıkların eylemlerinin TCK'nin 244/2-3. maddelerinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturup oluşturmadığı hususunun gerekçeli kararda tartışılması gerektiği gözetilmeden, eksik inceleme ile hükümler kurulması,

2-Kabul ve uygulamaya göre de;

5237 sayılı TCK'nin 40/2. maddesine göre, özgü suçlarda özel faillik niteliği taşıyan kişilerin fail olabileceği bu suçun işlenişine iştirak eden diğer kişilerin ise ancak azmettiren veya yardım eden olarak sorumlu tutulabileceği cihetle, sanık ...'un eyleminin TCK'nin 38/1 ve 40/2. maddeleri delaletiyle "memurun resmi belgede sahteciliği suçuna azmettirme suretiyle iştirak" suçunu oluşturacağı gözetilmeden, yazılı şekilde yardım eden sıfatıyla cezalandırılması suretiyle eksik ceza tayini,

Yasaya aykırı, sanık ... müdafii, sanıklar ... ve ...'un temyiz nedenleri bu itibarla yerinde görülmüş olduğundan, hükümlerin bu sebepten dolayı 5320 sayılı Kanun'un 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK'nin 321. maddesi uyarınca BOZULMASINA, 19.09.2019 tarihinde oybirliği ile karar verildi.

Kararda TCK'nin 244/2-3. maddelerinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturup oluşturmadığı hususunun gerekçeli kararda tartışılması gerektiği gözetilmeden, eksik inceleme ile hükümler kurulması nedeniyle yerel mahkeme kararının bozulmasına karar verilmiştir

KARAR 8:

T.C.
YARGITAY
15.Ceza Dairesi
Esas No: 2017/14178
Karar No: 2020/4067
Karar Tarihi: 01-06-2020

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine girme suçu – Sanıkların eyleminin 5237 sayılı kanunda düzenlenen suçu oluşturduğu gözetilmeden suç vasfında hataya düşülerek bilişim sistemine girme suçundan mahkumiyetlerine karar verildiği - Hükmün bozulması

ÖZET: Bilişim sistemine girme suçundan sanıklar ... ve ...'ın mahkumiyetine ilişkin hükümlerin temyiz incelenmesinde; Sanıkların ... Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp ücreti karşılığı yararlanmak yerine bir yazılım ile müşteki şirketin bilişim sistemine veri gönderip, seri şekilde milyonlarca sorgu yapıp sistemde var olan verileri aldıkları anlaşıldığından sanıkların eyleminin 5237 sayılı TCK'nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek bilişim sistemine girme suçundan mahkumiyetlerine karar verilmesi Bozmayı gerektirmiş, katılan kurumlar vekili ve o yer Cumhuriyet savcısının temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükümlerin bu sebepten dolayı 5320 sayılı Kanunun 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK'nın 321. maddesi uyarınca bozulmasına karar verilmiştir.

(5271 S. K. m. 223) (5237 S. K. m. 43, 52, 62, 243, 244) (1412 S. K. m. 317, 321)

Bilişim sistemlerine girme suçundan sanıklar ... ve ...'ın mahkumiyetine, sanık ...'nun beraatine ilişkin hükümler katılan kurumlar vekili, müşteki şirket vekili ve o yer Cumhuriyet savcısı tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü;

Müşteki ...Bilişim Çözümleri Ticaret Limited Şirketinin olay tarihinden önce 5490 sayılı Nüfus Kanununa göre hazırlanan Kimlik Paylaşım Sistemi Yönetmeliği ve Kimlik Paylaşım Sistemi Üzerinden Alınan Bilgilerin Ücretlendirilmesine İlişkin Esas ve Usuller Hakkında Tebliğ kapsamında bu sistemden ücreti karşılığı yararlanmak istediği, müşteki ...Bilişim Çözümleri Ticaret Limited Şirketi ile ... Nüfus ve Vatandaşlık İşler Genel Müdürlüğü arasında 09.05.2008 tarihinde imzalanan sözleşme ile kullanım hakkı aldığı, müşteki ...Bilişim Çözümleri Ticaret Limited Şirketinin Domain satışı ve Hosting hizmetleri yaptığı, işi gereği sistemine üye olmak isteyen müşteri kimliklerini doğrulatmak için sistemden yararlandığı, başka bir ifade ile www.isimtescil.net adlı bilişim sistemine internet üzerinden müşteri olmak isteyenlerin kimlikleri doğrulatılırken Mernis sistemi üzerinden belli sayıda sorguya müsaade edildiği, anlaşmaya göre Mernis sisteminden her bir sorgu karşılığı 0,02 TL. kamu maliyesi hesabına aylık olarak ödendiği, Sanık ...'nin nun ... Esnaf ve Sanatkârlar Odası başkanı, diğer sanıkların de odanın bilgi işlem kısmında çalışan elemanları oldukları, sanıkların ... Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek istedikleri, bunun için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp ücreti karşılığı yararlanmak yerine, bunu haksız şekilde yapmayı planladıkları, bunun için www.isimtescil.net bilişim sistemi ara yüzünden Mernis sistemindeki kimlik bilgilerini karşılıksız çekmek için bir yazılım hazırladıkları, bu düzeneği ... Esnaf ve sanatkarlar odasına ait bina içindeki sunucu üzerinde çalıştırıp milyonlarca sorgu gönderip Mernis'te kayıtlı verileri sürekli şekilde çektikleri, bu şekilde sanıkların üzerine atılı suçu işlediklerinin iddia edildiği somut olayda;

1-Müşteki ...Bilişim Çözümleri Ltd. Şti. vekilinin temyiz başvurusunun incelenmesinde;

29/06/2012 tarihli talimat duruşması ile usulüne uygun şekilde duruşmadan haberdar edilen müşteki vekilinin, talimat duruşma tutanağına göre müşteki vekilinin katılma talebinin bulunmadığı, herhangi bir mazeret bildirmeden duruşmalara katılmadığı gibi yazılı bir dilekçe ile davaya katılma talebinde de bulunmadığı, bu kapsamla katılan sıfatını elde edemediği anlaşılmakla, katılma ve hükmü temyiz etme yetkisi bulunmayan müşteki vekilinin temyiz talebinin CMUK 317. maddesi gereği REDDİNE,

2- Sanık ...'nun beraatine ilişkin hükmün temyiz incelenmesinde;

Sanık savunması, katılan ve müşteki beyanı, bilirkişi raporu ve tüm dosya kapsamından, sanığın üzerine atılı suçu işlediğinin sabit olmadığı gerekçelerine dayanan mahkemenin beraat hükmünde isabetsizlik görülmemiştir.

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre; katılan kurumlar vekili ve o yer Cumhuriyet savcısının yerinde görülmeyen temyiz itirazlarının reddiyle, hükmün ONANMASINA,

3-Bilişim sistemine girme suçundan sanıklar ... ve ...'ın mahkumiyetine ilişkin hükümlerin temyiz incelenmesinde;

Sanıkların ... Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp ücreti karşılığı yararlanmak yerine bir yazılım ile müşteki şirketin bilişim sistemine veri gönderip, seri şekilde milyonlarca sorgu yapıp sistemde var olan verileri aldıkları anlaşıldığından sanıkların eyleminin 5237 sayılı TCK'nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemine girme suçundan mahkumiyetlerine karar verilmesi

Bozmayı gerektirmiş, katılan kurumlar vekili ve o yer Cumhuriyet savcısının temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükümlerin bu sebepten dolayı 5320 sayılı Kanunun 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK'nın 321. maddesi uyarınca BOZULMASINA, 01/06/2020 tarihinde oybirliği ile karar verildi.

Kararda 5237 sayılı TCK'nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek bilişim sistemine girme suçundan

mahkumiyetlerine karar verilmesi hukuka aykırı olması nedeniyle yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 9:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2017/21566
Karar No: 2020/13171
Karar Tarihi: 11-06-2020

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim suçu – Sanıkların eylemlerinin 5237 sayılı kanunda tanımlanan kamu kurum ve kuruluşlarının zararına dolandırıcılık suçunu oluşturduğu – Hükmün bozulması

ÖZET: Sanıkların amaç ve kastının; hileli ve hukuka aykırı olarak katılan kurumun denetleme olanağını ortadan kaldıracak şekilde yükleme yapılan el kartların bayilere veya 3. şahıslara satılması suretiyle katılan belediyenin zararına kendilerine ise haksız yarar sağlamak olduğu ve bu nedenle sanıkların eylemlerinin 5237 sayılı TCK.nın 158/1-e maddesinde tanımlanan kamu kurum ve kuruluşlarının zararına dolandırıcılık suçunu oluşturmasına rağmen, uygulama yeri bulunmayan TCK.nın 244/4. maddesindeki bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun gösterilmesi suretiyle hüküm kurulması, Yasaya aykırı, sanıklar müdafilerinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükümlerin bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK.nın 321. ve 326/son maddeleri uyarınca ceza miktarı bakımından kazanılmış hakları saklı kalmak kaydıyla bozulmasına karar verilmiştir
(5237 S. K. m. 158, 244) (1412 S. K. m. 321, 326)

Gereği görüşülüp düşünüldü:

"Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir.

Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir.

Veri, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlarda dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgiyi ifade eder. (Sanal Ortamda İşlenen Suçlar Sözleşmesi madde 1, TBMM onay tarihi: 22.04.2014)

TCK.nın 244. maddesinin bir ve ikinci fıkralarında klasik mala zarar verme suçunun özel bir şekli düzenlenmiş 3. fıkrada nitelikli haline, 4. fıkrada ise haksız çıkar sağlanmasına yer verilmiştir. Maddede yazılı suçun oluşması için, bir bilişim sisteminin işleyişine yönelik engelleyici ve zarar verici fiiller bulunmalıdır. Diğer bir anlatımla bilişim sistemine yapılan müdahalelerle sistemin; veri işleme fonksiyonu yerine getirmesi engellenmeli, fonksiyonunu tamamen veya kısmen kaybetmeli veya verilere zarar verilmelidir.

Maddenin 4. fıkrasında kabul edilen bilişim sistemi aracılığıyla haksız yarar sağlama suçu, bileşik suç olup 1 ve 2. fıkrada yazılı suçların işlenerek bir çıkar sağlanması halinde gerçekleşecektir. Yani failin, bilişim sisteminin işleyişini engellemesi, bozması verileri yok etmesi, değiştirmesi, bozması, erişilmez kılınması, sisteme veri yerleştirip veya mevcut verileri başka yere göndermesi sonucu kendisine ya da bir başkasına haksız çıkar sağlaması hallerinde bu suç oluşacaktır.

Bu madde anlamında haksız çıkar yalnızca maddi yararları içermeyip, herhangi bir yararın elde edilmesi suçun oluşması için yeterlidir. Suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunu bilmesi gerekir. Buradaki haksızlık suçun maddi unsurlarından çıkara ilişkin bir nitelendirme olduğu için kusur değil, kast kapsamındadır ve suç kasten işlenebilir.

Maddede "başka bir suçu oluşturmaması halinde" denilerek "tali norm" niteliğinde bir düzenleme yapılmıştır. Ancak madde gerekçesinde, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir, denmiştir. Bilişim sistemleri aracılığıyla bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle

dolandırıcılık, zimmet gibi bir başka suçun oluşup oluşmadığı tartışılmalı eylem başka bir suçu oluşturmamışsa TCK.nın 244/4. maddesi irdelenmelidir.

Hile, Türk Dili Kurumu sözlüğünde; "birini aldatmak, yanıltmak için yapılan düzen, dolap, oyun, desise, entrika" şeklinde tanımlanmıştır. Uygulamadaki yerleşmiş kabule göre ise; "Hile nitelikli yalandır. Yalan belli oranda ağır, yoğun ve ustaca olmalı, sergileniş açısından mağdurun denetleme olanağını ortadan kaldırmalıdır. Kullanılan hile ile mağdur yanılgıya düşürülmeli ve yanıltma sonucu kandırıcı davranışlarla yalanlara inanan mağdur tarafından sanık veya başkasına haksız çıkar sağlanmalıdır... hileli davranışın aldatacak nitelikte olması gerekir. Basit bir yalan hileli hareket olarak kabul edilemez." biçiminde tanımlanmıştır. Yerleşmiş uygulamalar ve öğretideki baskın görüşlere göre ortaya konulan ilkeler gözönünde bulundurulduğunda; hile, maddi olmayan yollarla karşısındakini aldatan, yanılgıya düşüren, düzen, dolap, oyun, entrika ve bunun gibi her türlü eylem olarak kabul edilebilir. Bu eylemler bir gösteriş biçiminde olabileceği gibi, gizli davranışlar olarak da ortaya çıkabilir. Gösterişte, fail sahip bulunmadığı imkanlara ve sıfata sahip olduğunu bildirmekte, gizli davranışta ise kendi durum veya sıfatını gizlemektedir. Ancak sadece yalan söylemek, dolandırıcılık suçunun hile unsurunun gerçekleşmesi bakımından yeterli değildir. Kanun koyucu yalanı belirli bir takım şekiller altında yapıldığı ve kamu düzenini bozacak nitelikte bulunduğu hâllerde cezalandırmaktadır. Böyle olunca hukuki işlemlerde, sözleşmelerde bir kişi mücerret yalan söyleyerek diğerini aldatmış bulunuyorsa bu basit şekildeki aldatma, dolandırıcılık suçunun oluşumuna yetmeyecektir. Yapılan yalan açıklamaların dolandırıcılık suçunun hileli davranış unsurunu oluşturabilmesi için, bu açıklamaların doğruluğunu kabul ettirebilecek, böylece muhatabın inceleme eğilimini etkisiz bırakabilecek yoğunluk ve güçte olması ve gerektiğinde yalana bir takım dış hareketlerin eklenmiş bulunması gerekir. Esasen, hangi davranışların hileli olup olmadığı ve bu kapsamda değerlendirilmesi gerektiği yolunda genel bir kural koymak oldukça zor olmakla birlikte, olaysal olarak değerlendirme yapılmalı, olayın özelliği, mağdurun durumu, fiille olan ilişkisi, kullanılmışsa gizlenen veya değiştirilen belgenin nitelikleri ayrı ayrı nazara alınmak suretiyle sonuca ulaşılmalıdır.

TCK.nın 158/1-e bendinde belirtilen, kamu kurum ve kuruluşlarının zararına olarak dolandırıcılık suçunun işlenmesi, nitelikli hal kabul edilmiştir. Hangi kurum ve kuruluşların, kamusal nitelik taşıdığı, o kurumun kadro bakımından bağlı olduğu durumu düzenleyen mevzuata göre belirlenir. Bu nitelikli halin oluşması için, eylemin kamu kurum ve kuruluşlarının mal varlığına zarar vermek amacıyla işlenmesi gerekir. Zarar vermek, kamu kurum ve kuruluşlarından hakkı olmayan bir parayı almak yada bir borcu geri vermemek şeklinde olabilir. Bu suçun zarar göreni kamu kurum ve kuruluşunun tüzel kişiliğidir. Kamu kurum ve kuruluşlarının zarar görmesi söz konusu değilse bu suç oluşmayacaktır. Dolandırıcılık suçunun kamu yararına çalışan hayır kurumlarının zararına işlenmesi madde kapsamında değildir.

Bu açıklamalar ışığında oluşa ve tüm dosya kapsamına göre; sanık ...'in olay tarihinde katılan ... Belediyesine ait toplu taşıma araçlarında kullanılan ve sanık ...'dan satmak amacıyla aldığı el kartlardan 5 adetini tanesi 60 TL'den el kart dolum bayiliğini yapan tanık ...'a sattığı, tanık ...'ın da sanık ...'ten şüphelenerek durumu katılan kuruma bildirdiği ve tekrar sanık ...'e ulaşarak elinde başkaca el kart var ise 55 TL'den alacağını belirttiği, bunun üzerine sanık ...'in de sanık ...'dan aldığı 100 adet el kartı tanık ...'a satmak üzereyken kolluk görevlilerince yakalandığı, sanık ...'ın ise işyerinde yapılan aramada 327 adet el kartın ele geçirildiği, sanık ...'ın bu el kartları, sanık ...'dan 45.000 TL'lik alacağına karşılık sanık ... tarafından sanık ...'in ikametinden alınarak kendisine verildiğini beyan ettiği, ele geçirilen toplam 432 adet el kartın 15 adetinin katılan kurum sisteminde kaydının bulunduğu ve bu kartlara kovuşturma aşamasında alınan 11.04.2013 tarihli rapora göre; Konya 11. Asliye Ceza Mahkemesi'nin 2014/527 Esas, 2015/452 Karar sayılı dosyasında "bilişim sistemini kullanmak suretiyle haksız çıkar sağlama" suçundan yargılanan ...'nun işlettiği ve el kart dolum bayiliği yapan ... Büfe isimli işyerinde yer alan... nolu BSM cihazından kayıt dışı yükleme yapıldığı ve katılan kurumun 38.920 TL zarara uğradığı iddia olunan somut olayda; sanıkların aşamalardaki savunmaları ve 11.04.2013 tarihli, Konya 3. Asliye Hukuk Mahkemesi'nin 2010/193 Esas sayılı dosyasında alınan 31.07.2012 tarihli, Konya 11. Asliye Ceza Mahkemesi'nin 2014/527 Esas, 2015/452 Karar sayılı dosyasında soruşturma aşamasında düzenlenen 26.05.2010 havale tarihli bilirkişi raporlarında; BSM cihazının bayi tarafından bankaya kullanılacak bakiye yüklemesi yapıldıktan sonra bankanın katılan kuruma elektronik bildirimi üzerine bayinin BSM cihazıyla belediyeye bağlanmak suretiyle kart sahiplerine dolum yaptığının ve ... nolu BSM cihazına yüklenen

programın silindiğinin tespit edildiği ancak sanıkların cihazda yer alan yazılıma veya katılan kurumun sistemine müdahale ettiklerine dair bir tespitin bulunmaması, sanık ...'in soruşturma aşamasında müdafii huzurunda "...tanık ...'ın bürosunda bulunduğum sırada tanık ... veya sanık ...'den birisi müvekkillerinden alacaklarına karşı ellerinde el kartı olduğunu söyledi..." yönündeki beyanı da gözetildiğinde el kartların kayıt dışı yükleme yapıldıktan sonra sanıkların hüküm ve tasarrufuna geçmesi karşısında; sanıkların amaç ve kastının; hileli ve hukuka aykırı olarak katılan kurumun denetleme olanağını ortadan kaldıracak şekilde yükleme yapılan el kartların bayilere veya 3. şahıslara satılması suretiyle katılan belediyenin zararına kendilerine ise haksız yarar sağlamak olduğu ve bu nedenle sanıkların eylemlerinin 5237 sayılı TCK.nın 158/1-e maddesinde tanımlanan kamu kurum ve kuruluşlarının zararına dolandırıcılık suçunu oluşturmasına rağmen, uygulama yeri bulunmayan TCK.nın 244/4. maddesindeki bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun gösterilmesi suretiyle hüküm kurulması,

Yasaya aykırı, sanıklar müdafilerinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükümlerin bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK.nın 321. ve 326/son maddeleri uyarınca ceza miktarı bakımından kazanılmış hakları saklı kalmak kaydıyla BOZULMASINA, 11.06.2020 gününde oybirliği ile karar verildi.

Kararda TCK m. 244/4 gereğince hüküm kurulmasının yanlış olmasından dolayı yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 10:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2018/1078
Karar No: 2018/2485
Karar Tarihi: 08-03-2018

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine girme suçu – Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceğini savunduğu – Şikayetçinin girmediğini belirttiği sürede sanık tarafından E-posta adresine giriş yapılıp yapılmadığının tespiti gereği

ÖZET: Sanığın, şikayetçinin kullandığı e-posta adresi ile irtibatlı olan ... adresine bilgisi ve rızası olmaksızın şifreyi değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan hüküm kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Şikayetçinin bir aydır e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması yasaya aykırı olup hükmün bozulması gerekir.
(5237 S. K. m. 243)

Gereği görüşülüp düşünüldü:

Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş

yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (... vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin ve sanığa ait olduğu iddia olunan e-mail adresinin sanığa ve şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (İnternet Protokolu) numarası sorulmalıdır....'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikayetçinin e-mail adresine giriş yapıp yapmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikayetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikayetçi ve sanığın bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp ele geçirilen adresten bir başka adrese yazı veya görüntü gönderilmiş ise, bu olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri varsa tanık olarak dinlenmelidir.

Somut olayda; sanığın, şikayetçinin kullandığı ".....@hotmail. com" e-posta adresi ile irtibatlı olan ... adresine bilgisi ve rızası olmaksızın şifreyi değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan hüküm kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Şikayetçinin bir aydır e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması,

Yasaya aykırı, katılan vekilinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321. maddesi gereğince BOZULMASINA, 08.03.2018 gününde oybirliği ile karar verildi.

Kararda TCK m. 243 gereğince sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması yasaya aykırı olması nedeniyle yerel mahkemenin kararının bozulmasına karar verilmiştir.

KARAR 11:

T.C.
YARGITAY
12.Ceza Dairesi
Esas No: 2018/8586
Karar No: 2019/9340
Karar Tarihi: 25-09-2019

Bilişim sistemine girme suçu – Sanığa yüklenen suçların sanık tarafından işlendiğinin sabit olmadığı gerekçesiyle beraat kararı verilirken kanun madde ve fıkrasına uyulmaması – Hükmün düzeltilerek onanması

ÖZET: Sanığa yüklenen suçların sanık tarafından işlendiğinin sabit olmadığı gerekçesiyle beraat kararı verilirken, CMK'nın … madde, fıkra ve bendinin yanında, aynı Kanunun .. madde, fıkra ve bendinin de uygulama maddesi olarak yazılması suretiyle CMK'nın .. madde ve fıkrasına uyulmaması, bozmayı gerektirmiş, bozma nedeni yeniden yargılama yapılmasını gerektirmediğinden hükmün düzeltilerek onanması gerekmiştir.

(5237 S. K. m. 132, 243) (5271 S. K. m. 223)

Bilişim sistemine girme ve haberleşmenin gizliliğini ihlal suçlarından sanığın beraatine ilişkin hükümler, katılanlar vekili tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Mağdur ...'ın yetkilisi olduğu firmada finans müdürü olarak çalışmakta iken istifa eden ve daha sonra iş mahkemesinde işe iade davası açan sanık ...'ın, firmanın muhasebe müdürü olan diğer mağdur ...'e şirket tarafından tahsis edilen elektronik posta hesabına, yetkisiz erişim sağlayıp, mağdurlar arasındaki elektronik iletileri, kendi kullanımındaki elektronik posta hesabına gönderdikten sonra, söz konusu elektronik iletileri, iş mahkemesindeki dava dosyasına sunarak, TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ile TCK'nın 132/1 ve 132/2. madde ve fıkralarındaki haberleşmenin gizliliğini ihlal suçlarını işlediğinin iddia edildiği olayda;

Sanık ...'ın; bedelli askerlik uygulaması için firmadan 30.000,00 TL tutarında avans istediğini, kendisine yapılacak ödemenin kıdem tazminatına mahsuben yapılacağının, bu nedenle işten çıkış ve tekrar işe giriş yapılacağının söylendiğini, bu amaçla 31.08.2012 tarihinde istifa ettiğine dair dilekçeyi ve aynı tarihli ibranameyi imzaladığını, işten çıkarılmasına rağmen işe tekrar girişinin yapılmadığını, 17.09.2012 tarihinde ise hiçbir neden gösterilmeksizin iş akdinin fesh edilip, şirkete ait elektronik posta hesaplarına erişiminin de engellendiğini, 18-19.09.2012 tarihlerinde aynı departmanda beraber çalıştığı mağdur ...'ü telefonla arayıp, firmaya karşı dava açacağını, imzaladığı istifa dilekçesi ile ibranameyi ve konuya ilişkin firma ile arasında geçen elektronik iletileri istediğini, mağdur ...'ün "Beni bu işlere karıştırma, zaten benim elektronik posta adresimi biliyorsun, oradan girip al" dediğini, bunun üzerine 20-22.09.2012 tarihleri arasında mağdur ...'e şirket tarafından tahsis edilen elektronik posta hesabına önceden bildiği şifreyle giriş yapıp, temin ettiği istifa dilekçesi ve ibraname ile iddialarına ilişkin süreci destekler nitelikteki elektronik iletileri, iş mahkemesindeki 27.09.2012 tarihli dava dosyasına sunduğunu beyan etmesi, mağdur ...'ün, "... Murat ... şirketten ayrıldıktan sonra benimle ... irtibat kurarak kendisinin şirketteki görevinden tekrar geri işe alınacağı vaadiyle istifa ettiğini; fakat, işe alınmadığını, bu nedenle istifa dilekçesiyle ibranamesinin bir kopyasını istediğini söyledi, ben şirkette muhasebede personel işlerini takip ettiğim için bu belgelerin asıllarının benim erişimimde olduğunu biliyordu... kendisine bu durum şirketle senin aranda bir sorun, bu belgeleri sana veremem, bu durumu gerekirse patronlarla görüş dedim. Benim bu tavrım üzerine ... talep ettiği bu belgeleri bir şekilde ele geçireceğini ve ele geçirdikten sonra da benden aldığını söylemek suretiyle beni de zor durumda bırakacağını söyleyerek... benimle yaptığı görüşmeyi sonlandırdı. Aradan geçen bir süre sonra... şirket aleyhine açtığı iş mahkemesindeki davada benim şirket içerisinde kullandığım e-posta hesabıma yine şirket içerisindeki diğer kişilerle yaptığım özellikle şüpheliyi ilgilendiren e-posta ileti çıktılarının delil olarak sunulduğunu öğrendim. Ben şüpheliye hiçbir şekilde kullandığım e-posta hesabıma ait şifreleri vermedim. Nasıl öğrendiği konusunda da bilgim yoktur. Benim e-posta hesabıma ait şifrelerim kolay tahmin edilebilecek nitelikte de değildi; fakat, şüpheli belki benimle birlikte bulunduğu ortamlarda bu şifremi yazarken tespit etmiş olabilir. Benim e-posta hesabıma erişim

sağladıktan sonra herhangi bir değişiklik yapmamış, ben bu şekilde kullanmaya devam ettim, olaydan haberdar olunca şifremi değiştirerek güncelledim..."; "...sanığın üçüncü kişilerle yaptığım görüşmelere girip girmediğini tespit edemedim..." ve mağdur ...'ın "...Şirket dışından elektronik posta hesaplarına erişim yapabilmesi için öncelikle şirketimizin web sayfasına daha önceden tanımlanmış kullanıcı adı ve şifre kullanılarak giriş yapılması gerekmektedir. Soruşturma konusu elektronik posta yazışmaları ile ilgili şüpheli tarafından ne şekilde erişim sağlandığı araştırıldığında web sayfasına kendi kullanıcı adı ve şifresi ile giriş yaptıktan sonra Özgür'ün e-posta hesabına erişim sağladığını tespit ettik..." biçimindeki ifadelerinden, sanığın mağdur ...'ü telefonla arayıp öncelikle belge örneklerini ondan talep ettiğinin ve telefonda yaşanan tartışmaya rağmen mağdur ...'ün şifresini değiştirmemesinden dolayı onun şifresini bildiği elektronik posta hesabına girdiğinin anlaşılması, sanık tarafından açılan iş davasının reddine ilişkin yerel mahkeme kararının, Yargıtay 9. Hukuk Dairesinin 22.05.2014 tarihli, 2014/3243 esas, 2014/16502 karar sayılı ilamı ile "...Taraflar arasındaki uyuşmazlık davacının iş sözleşmesinin istifa ile sona erip ermediği noktasındadır. Somut olayda davalı davacının istifa ederek işten ayrıldığını davacının bedelli askerliğe müracaat ettiğini, bu kapsamda şirket tarafından kendisine 30.000 TL ödemede bulunulduğunu, davacının kendi işini kurmak amacıyla işten ayrıldığını belirterek davanın reddini talep etmiş, davacının 31.08.2012 tarihli istifa dilekçesini ve aynı tarihli ibranamesini sunmuştur. Davacı ise şirket tarafından kendisine ödenen bedelli askerlik tutarının kıdem tazminatı ödemesi olarak muhasebeleştirilmesi ve ilgili kayıtlara işlenebilmesi amacıyla giriş çıkış yapılması için söz konusu dilekçenin kendisinden alındığını iddia etmiştir. Gerçekten davalı tanığı ve çalışanı Özgür ... ifadesinde davacının iş akdinin feshedildiğini sonra işe geri alınmadığını, zannettiği kadarıyla davacı başvurmadığı için işe alınmadığını beyan ettiği, ayrıca davacının çıkışının dahi 31.08.2012 tarihi itibariyle değil istifa dilekçesi verildikten 17 gün sonra 17.09.2012 tarihinde yapıldığı, davalı davacı istifa dilekçesi verildikten sonra kendisiyle iki hafta daha çalışılması konusunda anlaşıldığını belirtmişse de bu konuda herhangi somut ve inandırıcı bir delil de sunulmadığı, sunulan dilekçede herhangi bir ihbar önelinin bulunmadığı, iş ilişkisi devam ederken bu şekilde alınan istifa dilekçesine itibar edilemeyeceği buna göre davacının iş sözleşmesinin işveren tarafından feshedildiği ancak feshin haksız ve geçersiz olduğu anlaşıldığından davanın kabulü yerine yazılı şekilde reddine karar verilmesi hatalıdır." gerekçesine dayalı olarak bozulması, dosyada mevcut iş mahkemesine sunulan elektronik iletilerin bir kısmının tarafı sanık olup, elektronik ileti içeriklerinin sanığın savunmasını doğrulaması, şikayete konu elektronik iletilerin üçüncü kişi ya da kişilerle paylaşıldığı ve/veya çoğaltılarak dağıtıldığına ilişkin bir iddianın olmaması karşısında, sanığın, kendisinin kandırılıp, istifa ettirilerek, iş akdinin haksız şekilde fesh edilmesinin ve yaşadığı süreci ispatlayan belgelerin tarafına verilmemesinin ardından, sadece kendisine ilişkin süreçle ilgili elektronik iletileri temin edip, iş mahkemesindeki iddialarını ispatlama ve kaybolma olasılığı bulunan delillerin muhafazasını sağlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle davranmadığına ve mağdur ...'ün rızasını alarak elektronik posta hesabına girdiğine dair savunmasının aksine, mahkumiyetine yeter, her türlü derecede şüpheden uzak, kesin ve inandırıcı delil bulunmaması nedeniyle sanık hakkında beraat kararı verilmesine ilişkin yerel mahkemenin kabulünde dosya kapsamına göre bir isabetsizlik görülmemiş; sanık hakkında bilişim sistemine girme ve haberleşmenin gizliliğini ihlal suçlarından mahkumiyet kararı verilmesi gerektiği düşüncesiyle beraat hükümlerinin bozulmasını öneren tebliğnamedeki görüşe iştirak edilmemiştir.

Mahkemece 26.01.2016 tarihinde tefhim edilen kararı yasal süresi içinde temyiz etmeyen sanık müdafii, 15.03.2016 tarihli temyize ve 09.01.2019 tarihli tebliğnameye cevap dilekçelerinde; hakkında beraat kararı verilen ve kendisini vekil ile temsil ettiren sanık yararına, hazine aleyhine, karar tarihinde yürürlükte bulunan Avukatlık Asgari Ücret Tarifesi gereğince maktu vekalet ücretine hükmedilmemesi nedeniyle hükümlerin düzeltilerek onanması gerektiğini ifade etmiş ve sanık lehine vekalet ücreti hükmolunmadığı anlaşılmış ise de, Yargıtay Ceza Genel Kurulunun 07.05.2013 tarihli, 2013/11-87-245 sayılı kararında da vurgulandığı üzere; vekalet ücreti kişisel hakka ilişkin olup, kişisel hakka ilişkin kanuna aykırılıkların Yargıtay tarafından bozma konusu yapılabilmesi için, hükmün karşı hak sahibi tarafından temyiz edilmiş olması gerektiğinden, temyiz edenin sıfatına göre, bu husus bozma sebebi olarak kabul edilmemiştir.

Adli emanete alınan 2 adet hard disk hakkında bir karar verilmemesi, bu konuda mahkemesinden her zaman bir karar alınması olanaklı olduğundan, bozma nedeni yapılmamıştır.

Yapılan yargılama sonunda, yüklenen suçların sanık tarafından işlendiğinin sabit olmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılanlar vekilinin sübuta, sanığa yüklenen suçların unsurlarının oluştuğuna, ele geçirilen elektronik iletilerin iş mahkemesindeki davayla ilgisi bulunmadığı gözetilmeden eksik incelemeyle karar verildiğine ilişkin sair temyiz itirazlarının reddine, ancak;

Sanığa yüklenen suçların sanık tarafından işlendiğinin sabit olmadığı gerekçesiyle beraat kararı verilirken, CMK'nın 223/2-e madde, fıkra ve bendinin yanında, aynı Kanunun 223/2-c madde, fıkra ve bendinin de uygulama maddesi olarak yazılması suretiyle CMK'nın 232/6. madde ve fıkrasına uyulmaması,

Kanuna aykırı olup, katılanlar vekilinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükümlerin bu nedenle 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince BOZULMASINA; ancak, yeniden yargılama gerektirmeyen bu konuda, aynı Kanunun 322. maddesi gereğince karar verilmesi mümkün bulunduğundan, aynı maddenin verdiği yetkiye istinaden; gerekçeli karardaki "sanığın CMK 223/2-c-e maddesi gereğince beraatine" ibarelerinin ve hüküm fıkrasının ilk paragrafının, "Sanık hakkında TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ile TCK'nın 132/1 ve 132/2. madde ve fıkralarındaki haberleşmenin gizliliğini ihlal suçlarından açılan davaların yapılan yargılaması sonunda, sanığa yüklenen suçların sanık tarafından işlendiğinin sabit olmadığı anlaşıldığından, CMK'nın 223/2-e madde, fıkra ve bendi gereğince sanığın beraatine" şeklinde değiştirilmesi suretiyle, eleştiri dışında, sair yönleri usul ve kanuna uygun bulunan hükümlerin DÜZELTİLEREK ONANMASINA, 25.09.2019 tarihinde oybirliğiyle karar verildi.

Kararda sanığın yüklenen suçların sanık tarafından işlendiğinin sabit olmaması nedeniyle verilen kararda kanun uygun madde ve fıkrasına dayanılmadığından yerel mahkeme kararının düzeltilerek onanmasına karar verilmiştir.

KARAR 12:

T.C.
YARGITAY
12.Ceza Dairesi
Esas No: 2019/13234
Karar No: 2023/1986
Karar Tarihi: 05-06-2023

Şantaj suçu – Mağdurun sanığın telefon konuşmasında kendisiyle yatması karşılığında mağdura ait eşyaların verileceğine yönelik soyut beyanı dışında şantaj suçundan cezalandırılmasına yeterli delil bulunmadığı – Hükmün bozulması

ÖZET: Dosya kapsamına, ikrar içeren savunmaya ve mağdur beyanına göre; sanık ile katılanın bir dönem duygusal arkadaşlık yaptıkları sıra da karşılıklı olarak sosyal paylaşım sitesi olan facebook şifrelerini verdikleri, mağduru ile sanığın ayrılması üzerine sanığın mağdura ait hesabın şifresini değiştirdiği iddia ve kabul eylemin 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrasında düzenlenen istemi engelleme bozma, verileri yok etme veya değiştirme suçunu oluşturduğu ve suçtan mahkumiyetine karar verilmesi gerekirken delillerin takdirinde hataya düşülerek ilgili şekilde verileri hukuk aykırı olarak verme veya ele geçirme suçundan mahkumiyete karar verilmesi hukuka aykırı görülmüştür. Mağdurun sanığın telefon konuşması sırasında kendisi ile yatması karşılığında sanıkta bulunan mağdura ait eşyaların verileceğine yönelik soyut beyanı dışında sanığın şantaj suçundan cezalandırılmasına yeterli her türlü şüpheden uzak kesin ve inandırıcı delil bulunmadığı anlaşılmakla sanık hakkında beraate karar verilmesi gerekirken ilgili şekilde 5237 sayılı Kanun'un 107 nci maddesin temel cezanın hapis ve adli para cezası birlikte düzenlenmesine

rağmen temel cezanın adli para cezası olarak belirlenmesi suretiyle mahkumiyete karar verilmesi hukuka aykırı bulunmuştur.

(1412 S. K. m. 305, 310, 317, 321) (5271 S. K. m. 260) (5237 S. K. m. 107, 136, 244)

DAVA:

Sanık hakkında kurulan hükümlerin; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 inci maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Ceza Muhakemesi Kanunu'nun (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

KARAR:

I. HUKUKÎ SÜREÇ

1. Erbaa 1. Asliye Ceza Mahkemesinin, 29.06.2015 tarihli ve 2015/271 Esas, 2015/608 Karar sayılı kararı ile sanık hakkında;

Verileri hukuka aykırı olarak verme veya ele geçirme suçundan 5237 sayılı Türk Ceza Kanunu'nun 136 ncı maddesinin birinci fıkrası, 62 nci maddesi, 53 üncü maddesi ve 51 inci maddesi uyarınca 1 yıl 8 ay hapis cezası ile cezalandırılmasına, hak yoksunluklarına ve ertelemeye,

Şantaj suçundan 5237 sayılı Kanun'un 107 nci maddesinin birinci fıkrası, 62 nci maddesi, 52 nci maddesi uyarınca 6.000,00 TL adli para cezası ile cezalandırılmasına,

Karar verilmiştir.

2. Dava dosyası, Yargıtay Cumhuriyet Başsavcılığınca düzenlenen 24.05.2019 tarihli ve 2016/324120 sayılı, verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan hükmün onanması, şantaj suçundan kurulan hükmün ise katılanın soyut iddiası dışında delil bulunmadığı gerekçesi ile hükmün bozulması görüşünü içerir Tebliğname ile Yargıtay 4. Ceza Dairesine tevdi edilmiştir.

3. Yargıtay 4. Ceza Dairesinin 12.09.2019 tarihli ve 2019/4002 Esas, 2019/13613 Karar sayılı görevsizlik kararı ile Dairemize gönderilmiştir.

II. TEMYİZ SEBEPLERİ

Sanığın temyiz isteği, verilen cezanın fazla olduğuna ilişkindir.

III. OLAY VE OLGULAR

1. Sanık ile mağdurun bir dönem duygusal arkadaşlık yaptıkları, arkadaşlıkları sırasında mağdurun kendisine ait facebook hesap şifresini sanığa verdiği, mağdurun sanıktan ayrılması üzerine sanığın kendisinde bulunan şifreyi kullanarak mağdura ait facebook hesabının şifresini değiştirip mağdurun girişini engellediği, mağdur ile yaptığı telefon konuşması sırasında kendisi ile yattığı takdirde kendisinde mağdura ait olan her şeyi vereceğini söylediği iddiası ile sanık hakkında sistemi engelleme bozma, verileri yok etme veya değiştirme ve şantaj suçlarından kamu davası açılmıştır.

2. Mahkemece sanığın mağdura ait hesabın şifresini değiştirme eyleminin 5237 sayılı Kanun'un 136 ncı maddesinin birinci fıkrasında düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu kabul edilerek sanık hakkında ek savunma hakkı tanınıp, sanığın mağdura şantajda bulunduğu kabul edilerek verileri hukuka aykırı olarak verme veya ele geçirme ve şantaj suçlarından mahkumiyete karar verilmiştir.

3. Sanık soruşturma ve kovuşturma sırasında, mağdur ile bir dönem arkadaşlık yaptıklarını, mağdurun hesabının şifresini verdiğini, kendisininde mağdura verdiğini, mağdurun başkaları ile konuşması üzerine ayrıldıklarını, mağdura ait hesabın şifresini değiştirdiğini ancak şantajda bulunmadığını savunmuş, mağdura ait hesap şifresini kolluk aşamasında kolluk görevlileri vasıtası ile mağdura iade etmiş, duruşma sırasında mağdura ait kendisinde bulunan resimleri mağdura iade etmiştir.

4. Mağdur soruşturma ve kovuşturma aşamasında sanık ile arkadaşlık yaptığını, karşılıklı olarak şifre verdiklerini, daha sonra sanıktan ayrılması üzerine sanığın şifreyi değiştirdiğini, facebook üzerinde mesajlaştıkların şartı olduğunu söylediğini, telefon ile aradığı sırada kendisi ile yatması durumunda resimlerini vereceğini söylediğini beyan etmiş, duruşmada sanığın ceza almasını istemediğini beyan ederek şikayetinden vazgeçmiştir.

IV. GEREKÇE

1. Dosya kapsamına, ikrar içeren savunmaya ve mağdur beyanına göre; sanık ile katılanın bir dönem duygusal arkadaşlık yaptıkları sıra da karşılıklı olarak sosyal paylaşım sitesi olan facebook şifrelerini verdikleri, mağduru ile sanığın ayrılması üzerine sanığın mağdura ait hesabın şifresini değiştirdiği iddia ve kabul eylemin 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrasında düzenlenen istemi engelleme bozma, verileri yok etme veya değiştirme suçunu oluşturduğu ve suçtan mahkumiyetine karar verilmesi gerekirken delillerin takdirinde hataya düşülerek yazılı şekilde verileri hukuk aykırı olarak verme veya ele geçirme suçundan mahkumiyete karar verilmesi hukuka aykırı görülmüştür.

2. Mağdurun sanığın telefon konuşması sırasında kendisi ile yatması karşılığında sanıkta bulunan mağdura ait eşyaların verileceğine yönelik soyut beyanı dışında sanığın şantaj suçundan cezalandırılmasına yeterli her türlü şüpheden uzak kesin ve inandırıcı delil bulunmadığı anlaşılmakla sanık hakkında beraate karar verilmesi gerekirken yazılı şekilde 5237 sayılı Kanun'un 107 nci maddesin temel cezanın hapis ve adli para cezası birlikte düzenlenmesine rağmen temel cezanın adli para cezası olarak belirlenmesi suretiyle mahkumiyete karar verilmesi hukuka aykırı bulunmuştur.

SONUÇ:

I. KARAR

Gerekçe bölümünde açıklanan nedenlerle Erbaa 1. Asliye Ceza Mahkemesinin, 29.06.2015 tarihli ve 2015/271 Esas, 2015/608 Karar sayılı kararına yönelik sanığın temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 inci maddesi gereği, Tebliğname'ye kısmen uygun olarak, oy birliğiyle BOZULMASINA,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 05.06.2023 tarihinde karar verildi.

Kararda 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrasında düzenlenen istemi engelleme bozma, verileri yok etme veya değiştirme suçunu oluşturduğu ve suçtan mahkumiyetine karar verilmesi gerekirken delillerin takdirinde hataya düşülerek ilgili şekilde verileri hukuk aykırı olarak verme veya ele geçirme suçundan mahkumiyete karar verilmesi hukuka aykırı görülmesi nedeniyle yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 13:

T.C.
YARGITAY
2. Ceza Dairesi
Esas No: 2019/1560
Karar No: 2019/8994
Karar Tarihi: 16-05-2019

Banka veya kredi kartlarının kötüye kullanılması suçu – Bozma üzerine yapılan duruşmaya toplanan delillere gerekçeye Hakimin kanaat ve takdirine göre temyiz itirazlarının yerinde olmadığından reddi- Hükmün onanması

ÖZET: Sanıklar ..., ..., ..., ..., ..., ..., ... ve ... hakkında müştekiler ..., ..., ...,...Seyahat Turizm AŞ, ..., ... Bilişim AŞ., ... ve ...'e yönelik hırsızlık ve... ibareli kartın manyetik şeridine şikayetçi Türkiye... Bankasına ait kartın seri numaralarının kopyalanması ve sahte kredi kartı üretilmesi suretiyle banka veya kredi kartlarının kötüye kullanılması suçlarından; sanık ... hakkında müşteki ...'a yönelik hırsızlık; sanıklar ... ve ... hakkında müşteki ...'a yönelik hırsızlık; sanık ... hakkında... ibareli kartın manyetik şeridine şikayetçi Türkiye ... Bankasına ait kartın seri numaralarının kopyalanması ve sahte kredi kartı üretilmesi suretiyle banka veya kredi kartlarının kötüye kullanılması suçundan kurulan hükümlere yönelik temyiz istemlerinin incelenmesinde; bozma üzerine yapılan duruşmaya, toplanan delillere, gerekçeye, hakimin kanaat ve takdirine göre temyiz itirazları yerinde olmadığından reddiyle hükümlerin istem gibi onanmasına karar verilmiştir.

(5237 S. K. m. 243) (1412 S. K. m. 317) (5271 S. K. m. 231)

Dava: Dosya incelenerek gereği düşünüldü;

Her ne kadar hakkında 30/12/2008 tarihli karar ile hakkında suç işlemek amacıyla kurulan örgüte üye olma, hırsızlık, bilişim sistemine hukuka aykırı olarak girme suçlarından mahkumiyet kararları verilip, bu kararların temyiz edilmeksizin kesinleştiği hükümlü ...'ın 01/04/2019, 24/04/2019 ve 25/04/2019 tarihli dilekçeler ile yargılamanın yenilenmesi ve infazın durdurulması talepli dilekçeler göndermiş ise de; hükümlünün bahse konu dilekçeleri ile benzer mahiyetteki yargılamanın yenilenmesi ve infazın durdurulması talepli dilekçeleri üzerine daha önce Üsküdar(Kapatılan) 6. Asliye Ceza Mahkemesinin 28/02/2013 tarihli ek kararıyla taleplerin reddine karar verildiği, yine hükümlünün benzer talepleri üzerine Dairemizin 11/03/2015 tarih ve 2015/5295 E.-2015/5161 K. sayılı ilamı ile kanun yararına bozma talebinin reddine karar verildiğinin anlaşılması karşısında, hükümlünün yargılamanın yenilenmesi isteğine ilişkin 01/04/2019, 24/04/2019, 25/04/2019 tarihli dilekçeleri hakkında mahallinde işlem yapılmasının ve sanıklar ..., ..., ..., ..., ..., ..., ... ile ... hakkında 08/02/2008 tarihli iddianame ile TCK'nın 243/1. maddesinde düzenlenen bilişim sistemine hukuka aykırı olarak girme suçundan cezalandırılmaları istemiyle kamu davası açıldığı halde, bu suçla ilgili karar verilmediği anlaşılmakta ise de, zamanaşımı süresi içerisinde karar verilmesinin olanaklı olduğu kabul edilerek yapılan incelemede;

Karar: 1-Sanık ... hakkında bilişim sistemine hukuka aykırı olarak girme suçundan verilen hüküm kurulmasına yer olmadığına dair karara yönelik temyiz isteminin incelenmesinde;

Sanık ... hakkında, 08/02/2008 tarihli iddianame ile bilişim sistemine hukuka aykırı olarak girme suçundan da cezalandırılması talep edilerek kamu davası açıldığı halde, atılı suçtan hüküm kurulmamış ise de, mahkemesince sanık hakkında bu suçtan zamanaşımı içerisinde hüküm kurulması mümkün olup, ortada incelenecek bir hüküm bulunmadığından, sanık müdafiinin konusu bulunmayan temyiz isteminin 5320 sayılı Kanun'un 8/1. maddesinin yollaması ile 1412 sayılı CMUK'nın 317. Maddesi uyarınca REDDİNE,

2-Sanıklar ..., ..., ..., ..., ..., ..., ... ve ... hakkında müşteki ...'a yönelik resmi belgede sahtecilik; müşteki ... ve ...'a yönelik banka veya kredi kartlarının kötüye kullanılması suçlarından; sanık ... hakkında müşteki ...'ya yönelik, sanık ... hakkında müşteki ...'a yönelik hırsızlık suçundan verilen hükmün açıklanmasının geri bırakılmasına dair kararlara yönelik temyiz isteminin incelenmesinde;

Sanıklar ..., ..., ..., ..., ..., ..., ... ve ... hakkında müşteki ...'a yönelik resmi belgede sahtecilik; müşteki ... ve ...'a yönelik banka veya kredi kartlarının kötüye kullanılması suçlarından; sanık ... hakkında müşteki...'ya yönelik, sanık ... hakkında müşteki ...'a yönelik hırsızlık suçundan verilen hükmün açıklanmasının geri bırakılmasına dair kararların, 5271 sayılı CMK'nın 231/12. maddesi uyarınca itiraza tabi olduğu, bu kararların temyizi mümkün olmadığından, 5271 sayılı CMK'nın 264. maddesine göre de, kanun yolunun ve merciinin belirlenmesinde yanılma, başvuranın hakkını ortadan kaldırmayacağından, sanık ... ve müdafii, sanık ... ve müdafii, sanık ..., sanık ..., sanık ... ve müdafii, sanık ... ve müdafii, sanık ..., sanık ... ve müdafii, sanık ..., sanık ...'ın dilekçesi itiraz niteliğinde kabul edilerek itirazın merciince incelenmesi için dosyanın incelenmeksizin istem gibi mahalline İADESİNE,

3-Sanıklar ..., ..., ..., ..., ..., ..., ... ve ... hakkında müştekiler ..., ..., ...,...Seyahat Turizm AŞ, ..., ... Bilişim AŞ., ... ve ...'e yönelik hırsızlık ve... ibareli kartın manyetik şeridine şikayetçi Türkiye... Bankasına ait kartın seri numaralarının kopyalanması ve sahte kredi kartı üretilmesi suretiyle banka veya kredi kartlarının kötüye kullanılması suçlarından; sanık ... hakkında müşteki ...'a yönelik hırsızlık; sanıklar ... ve ... hakkında müşteki ...'a yönelik hırsızlık; sanık ... hakkında... ibareli kartın manyetik şeridine şikayetçi Türkiye ... Bankasına ait kartın seri numaralarının kopyalanması ve sahte kredi kartı üretilmesi suretiyle banka veya kredi kartlarının kötüye kullanılması suçundan kurulan hükümlere yönelik temyiz istemlerinin incelenmesinde;

Sonuç: Bozma üzerine yapılan duruşmaya, toplanan delillere, gerekçeye, hakimin kanaat ve takdirine göre temyiz itirazları yerinde olmadığından reddiyle hükümlerin istem gibi ONANMASINA, 16/05/2019 tarihinde oy birliğiyle karar verildi.

Kararda TCK m. 243/1 düzenlenen Bilişim Sistemine Hukuka Aykırı olarak Girme suçundan Türkiye ... Bankasına ait kartın seri numaralarının kopyalanması ve sahte kredi

kartı üretilmesi suretiyle banka veya kredi kartlarının kötüye kullanılması suçundan kurulan hükümlere yönelik temyiz istemlerinin incelenmesinde; bozma üzerine yapılan duruşmaya, toplanan delillere, gerekçeye, hakimin kanaat ve takdirine göre temyiz itirazları yerinde olmadığından reddiyle hükümlerin istem gibi onanmasına karar verilmiştir.

KARAR 14:

T.C.
YARGITAY
12..Ceza Dairesi
Esas No: 2020/892
Karar No: 2022/3902
Karar Tarihi: 18-05-2022

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçu – Sistemi engelleme bozma verileri yok etme veya değiştirme suçunu işlediği iddiası ile ek savunma hakkı verilmeden temel cezada yarı oranında artırım yapılması – Hükmün bopzulmasıI

ÖZET: Sanık mağdura tahsis edilen Elektronik Kamu Alımları Platformu (EKAP) kullanıcı adı ve şifresi ile Kamu İhale Kurumuna ait bilişim sistemine hukuka aykırı olarak giriş yapıp, Pozantı Belediyesi tarafından yapılması kararlaştırılan hizmet alımı ihalesini iptal etmesi nedeniyle TCK'nın 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu işlediği iddiasına konu olayda iddianamede uygulanması talep edilmediği halde ek savunma hakkı verilmeden TCK'nın 244/3. madde ve fıkrası uyarınca temel cezada yarı oranında artırım yapılması suretiyle CMK'nın 226. maddesine uyulmaması kanuna aykırı olup hükmün bozulmasını gerektirmiştir.

(5320 S. K. m. 8) (1412 S. K. m. 317, 321) (5237 S. K. m. 53, 136, 244) (5271 S. K. m. 226, 232) (ANY. MAH. 08.10.2015 T. 2014/140 E. 2015/85 K.) (YCGK 11.04.2000 T. 200/4-65 E. 2000/69 K.) (YCGK 22.10.2002 T. 2002/4-234 E. 2002/366 K.) (YCGK 04.07.2006 T. 2006/5-127 E. 2006/180 (YCGK 03.05.2011 T. 2011/4-155 E. 2011/80 K.) (YCGK 21.02.2012 T. 2012/8-279 E. 2012/55 K.) (YCGK 15.04.2014 T. 2014/4-599 E. 2014/190 K) (YCGK 25.03.2003 T. 2003/5-41 E. 2003/54 K.)

Dava: Verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanıklar ... ile ...'ın beraatlerine ve sanık ...'nin mahkumiyetine, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan sanık ...'nin mahkumiyetine ilişkin hükümler, sanık ... müdafii tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Karar: Dairemizin 19.02.2020 tarihli tevdii kararı uyarınca, Yargıtay Cumhuriyet Başsavcılığı tarafından sanık ...'nin sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mahkumiyetine ilişkin hükme yönelik sanık ...müdafinin temyizi ile ilgili olarak görüş içeren ek tebliğnamenin düzenlendiği belirlenerek yapılan incelemede:

İddianamedeki anlatıma ve uygulanması istenen sevk maddelerine göre; sanıklar ... ve ... hakkında sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan da davalar açılmasına rağmen mahkemece adı geçen sanıklara yüklenen bu suça ilişkin davalarla ilgili olarak hüküm kurulmadığı anlaşıldığından, sanıklar ... ve ...'ın dava konusu edilen bu eylemleri hakkında, UYAP sisteminden temin edilen nüfus kayıt örneğinde sanık R.'ın 23.07.2017 tarihinde temyiz aşamasında öldüğünün tespit edildiği de dikkate alınıp, zamanaşımı süresi içinde bir karar verilmesi mümkün görülmüştür.

A) Sanıklar ... ve ... hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan beraat hükümlerine yönelik temyiz isteminin incelenmesinde; Mağdur kavramı gibi kanunda açıkça tanımlanmamış olan "suçtan zarar görme" kavramının, gerek Ceza Genel Kurulu gerek Özel Dairelerin yerleşmiş kararlarında; "suçtan doğrudan doğruya zarar görmüş bulunma hali" olarak anlaşılıp uygulandığı, buna bağlı olarak da dolaylı veya muhtemel zararların, davaya katılma hakkı vermeyeceğinin kabul edildiği, bu

hususun, Ceza Genel Kurulunun 11.04.2000 tarihli ve 65-69, 22.10.2002 tarihli ve 234-366, 04.07.2006 tarihli ve 127-180, 03.05.2011 tarihli ve 155-80, 21.02.2012 tarihli ve 279-55, 15.04.2014 tarihli ve 599-190, 28.03.2017 tarihli ve 214-206 Sayılı kararlarında; "dolaylı veya muhtemel zarar, davaya katılma hakkı vermez" şeklinde açıkça ifade edildiği ve Ceza Genel Kurulunun 25.03.2003 tarihli ve 41-54 Sayılı kararında da "tazminat ödenmesi, itibar zedelenmesi ve güven kaybı" gibi dolaylı zararlara dayanarak kamu davasına katılmanın olanaklı olmadığının kabul edilmesi karşısında, sanıklar ... ve ... hakkında mağdur O.'a yönelik verileri hukuka aykırı olarak verme veya ele geçirme suçundan açılan kamu davasında; sanıklar ... ve ...'a atılı suçun koruduğu hukuki yarar ve niteliği itibariyle aynı mağdura yönelik aynı suçtan yargılanan sanık ...'nin diğer sanıklar ... ve ...'a yüklenen suçun mağduru olmadığı ve suçtan doğrudan zarar görmemesi nedeniyle davaya katılmasına ilişkin hakkında verilmiş bir karar da bulunmadığı anlaşıldığından, sanık ...müdafinin sanıklar ... ve ... hakkındaki beraat hükümlerine yönelik temyiz isteminin 5320 Sayılı Kanun'un 8. maddesi uyarınca halen uygulanmakta olan 1412 Sayılı CMUK'un 317. maddesi gereğince isteme aykırı olarak REDDİNE

B) Sanık ... hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan mahkumiyet hükmüne yönelik temyiz isteminin incelenmesinde;

Sanık ...'nin, mağdur O.'a ait Elektronik Kamu Alımları Platformu (EKAP) kullanıcı adı ve şifresini, onun bilgisi ve rızası olmaksızın ele geçirmesi biçiminde sübut bulan eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna dair yerel mahkemenin kabulünde dosya kapsamına göre bir isabetsizlik görülmemiştir.

Sanık ... hakkında kasten işlemiş olduğu suçtan dolayı hapis cezasına mahkumiyetin kanuni sonucu olarak TCK'nın 53/1. madde ve fıkrasında öngörülen hak yoksunluklarına hükmedilmemesi isabetsizliği, T.C. Anayasa Mahkemesi'nin 24.11.2015 tarihli ve 29542 Sayılı Resmi Gazetede yayımlanan 2014/140 Esas - 2015/85 Karar sayılı iptal kararı da gözetilerek infaz aşamasında dikkate alınabileceğinden, bu nedenle hükmün bozulmasını öneren tebliğnamedeki görüşe iştirak edilmemiştir.

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, sanık ...müdafinin suçun yasal unsurlarının oluşmadığına, ceza miktarına, hükmedilen hapis cezasının seçenek yaptırımlara çevrilmemesine ilişkin temyiz itirazlarının reddiyle, hükmün isteme aykırı olarak ONANMASINA,

C) Sanık ... hakkında sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan kurulan mahkumiyet hükmüne yönelik temyiz isteminin incelenmesine gelince;

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, sanık ...müdafinin sair temyiz itirazlarının reddine, ancak;

1) Dosya kapsamına göre; 13.02.2015 olan suçun işlendiği tarihin, gerekçeli karar başlığına, "2015" olarak eksik yazılması suretiyle CMK'nın 232/2-c. madde, fıkra ve bendine uyulmaması,

2) Sanık ...'nin, mağdur O.'a tahsis edilen Elektronik Kamu Alımları Platformu (EKAP) kullanıcı adı ve şifresi ile Kamu İhale Kurumuna ait bilişim sistemine hukuka aykırı olarak giriş yapıp, Pozantı Belediyesi tarafından 13.02.2015 günü saat 10.00'da yapılması kararlaştırılan hizmet alımı ihalesini iptal etmesi nedeniyle TCK'nın 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu işlediği iddiasına konu olayda;

İddianamede uygulanması talep edilmediği halde ek savunma hakkı verilmeden TCK'nın 244/3. madde ve fıkrası uyarınca temel cezada yarı oranında artırım yapılması suretiyle CMK'nın 226. maddesine uyulmaması,

Sonuç: Kanuna aykırı olup, sanık ...müdafinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu nedenlerle 5320 Sayılı Kanun'un 8. maddesi uyarınca halen uygulanmakta olan 1412 Sayılı CMUK'un 321. maddesi gereğince isteme aykırı olarak BOZULMASINA, 18.05.2022 tarihinde oybirliğiyle karar verildi.

Kararda TCK'nın 244/3. madde ve fıkrası uyarınca temel cezada yarı oranında artırım yapılması suretiyle CMK'nın 226. maddesine uyulmaması kanuna aykırı olup yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 15:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2020/11243
Karar No: 2023/118
Karar Tarihi: 18-01-2023

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Sistemi engelleme bozma verileri yok etme veya değiştirme suçu – Sanığın mağdura ait ad soyad ve fotoğrafı kullanmak şeklindeki eylemi – Suç vasfında yanılgıya düşülerek hüküm kurulmasının isabetsizliği – Hükmün bozulduğu

ÖZET: Somut olayda, mağdurun, Facebook adllı bilişim sistemi içinde kendisi tarafından oluşturulan bir sayfası bulunmaması nedeniyle bu suçun oluşmadığı, sanığın mağdura ait ad, soyad ve fotoğrafı kullanmak şeklindeki eyleminin 5237 sayılı Kanun'un 136 ncı maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçunu oluşturduğu anlaşılmakla suç vasfında yanılgıya düşülerek hüküm kurulması hukuka uygun bulunmamıştır.
(5237 S. K. m. 53, 136, 244)

Sanık hakkında kurulan hükmün; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 ... maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 ... maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Ceza Muhakemesi Kanunu'nun (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

Sanık hakkında sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan açılan davada, ... 2. Asliye Ceza Mahkemesinin, 31.12.2015 tarihli kararı ile sanık hakkında sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 244 üncü maddesinin ikinci fıkrası ve 53 üncü maddesinin birinci fıkrası uyarınca 6 ay hapis cezası ile cezalandırılmasına ve hak yoksunluklarına karar verilmiştir.

II.TEMYİZ SEBEPLERİ

Sanığın temyiz isteği; eksik araştırma yapıldığına, delillerin hatalı değerlendirildiğine, bilirkişi raporunun güvenilir olmadığına, usul ve yasaya aykırı karar verildiği ve benzeri itirazlara ilişkindir.

III. OLAY VE OLGULAR

1. Davaya konu olay, sanığın mağdura ait fotoğraf, ad ve soyadı kullanarak açtığı facebook hesabı üzerinden mağdurun arkadaşları ile cinsel içerikli yazışmalar yaptığı iddiasına ilişkindir.

2. İzmir Emniyet Siber Suçlarla Mücadele Adli Bilişim Büro Amirliğince düzenlenen 27.04.2015 tarihli inceleme raporunda; sanıktan elde edilen bilgisayar hardiskinde facebok internet sayfasından kullanıcı hesabının açıldığı ve ... ... isimli kullanıcı ile görüşme yapıldığına dair tespit yapılamadığı, ... isimli şahsa ait facebook üzerinde oluşturulan kullanıcı hesabı olduğu ve bu hesabı görüntüleyerek buradan mağdur ...'nun fotoğraflarına, arkadaşlarına ve kullanıcısı tarafından görüntülenmesine izin verilen bilgilerin görüntülendiği değerlendirilmiştir.

3. Mağdur ad, soyad ve fotoğrafı ile açılan sahte facebook hesabı ekran görüntüsü ve mağdurun arkadaşı ... ile sanığın facebook üzerinden yazışmalarına ilişkin ekran görüntüsü 01.08.2012 ve 02.08.2012 tarihli tutanaklar ile tespit edilmiştir.

4. Tanık F.Y., mağdur ... izindeyken mağdurun facebook hesabından kendisine mesaj gelmesi üzerine yazışmaya başladığını, bir süre sonra cinsel içerikli mesajlar gelmeye başlayınca, karşıdaki şahsın arkadaşı ... olmadığını anladığı ve mağdur ...'yu durumdan haberdar ettiğini beyan etmiştir.

5. Sanığın, 01.07.2012 tarihinde mağduru birçok defa aradığına ilişkin HTS kayıtları dosyada mevcuttur.

6. Facebook vekili tarafından gönderilen 04.09.2012 tarihli cevap yazısında, bilgi yetersizliği nedeniyle ... ... ismi ile oluşturulan profil tespit edilemediği, söz konusu profilin şirket kullanım koşullarına uygunluğunun incelenmesi amacıyla tespit edilebilmesi için talepte belirtilen sayfanın bağlantı adresinin veya söz konusu profil oluşturulurken kullanılan e-posta adres bilgilerinin gönderilmesi gerektiği bildirilmiştir.

7. Sanık üzerine atılı suçu işlemediğini beyan etmiştir.

II.GEREKÇE

5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrasında düzenlenen suçun uygulanabilmesi için, mağdurun bir bilişim sisteminin bulunması, failin de bu bilişim sistemine hukuka aykırı girerek, bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme seçimlik hareketlerden birini yapması gerekmektedir.

Somut olayda, mağdurun, Facebook adllı bilişim sistemi içinde kendisi tarafından oluşturulan bir sayfası bulunmaması nedeniyle bu suçun oluşmadığı, sanığın mağdura ait ad, soyad ve fotoğrafı kullanmak şeklindeki eyleminin 5237 sayılı Kanun'un 136 ncı maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçunu oluşturduğu anlaşılmakla suç vasfında yanılgıya düşülerek hüküm kurulması hukuka uygun bulunmamıştır.

III.KARAR

Gerekçe bölümünde açıklanan nedenlerle ... 2. Asliye Ceza Mahkemesinin, 31.12.2015 tarihli ve 2014/4 Esas, 2015/775 Karar sayılı kararına yönelik sanığın temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 ... ve 326 ıncı maddenin son fıkrası gereği, Tebliğnameye uygun olarak, oy birliğiyle BOZULMASINA,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 18.01.2023 tarihinde karar verildi.

Kararda TCK m. 244 gereğince Facebook adlı bilişim sistemi içinde kendisi tarafından oluşturulan bir sayfası bulunmaması nedeniyle bu suçun oluşmadığı, sanığın mağdura ait ad, soyad ve fotoğrafı kullanmak şeklindeki eyleminin 5237 sayılı Kanun'un 136 ncı maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçunu oluşturduğu anlaşılmakla suç vasfında yanılgıya düşülerek hüküm kurulması hukuka uygun bulunması nedeniyle yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 16:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2020/11287
Karar No: 2023/23
Karar Tarihi: 12-01-2023

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçu - Eyleme uyan suç vasfı ile yaptırımların doğru biçimde belirlendiği – Sanığın temyiz itirazı yönünden hükümde hukuka aykırılık görülmediği - Hükmün onandığı

ÖZET: Dosyadaki olay ve olgular karşısında, sanığın savunmasına itibar edilmemiştir. Mahkemenin suçun sübutu ve nitelendirmesinde isabetsizlik görülmemiştir. Yargılama sürecindeki işlemlerin usul ve kanuna uygun olarak yapıldığı, aşamalarda ileri sürülen iddia ve savunmaların toplanan tüm delillerle birlikte gerekçeli kararda tartışıldığı, tanık A.A. tarafından işletilen internet kafeden şikayetçinin bilişim sistemine girmek suretiyle eylemin sanık tarafından gerçekleştirildiği, vicdanî kanının dosya içindeki belge ve bilgilerle uyumlu olarak kesin verilere dayandırıldığı, eyleme uyan suç vasfı ile yaptırımların doğru biçimde belirlendiği anlaşıldığından, sanığın temyiz itirazı yönünden hükümde hukuka aykırılık görülmemiştir.

(5237 S. K. m. 53, 58, 244) (5271 S. K. m. 253)

Sanık hakkında kurulan hükmün; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 ... maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 ... maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Ceza Muhakemesi Kanunu'nun (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

1. Sanık hakkında bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan dava açılmıştır.

2. Finike Asliye Ceza Mahkemesinin, 15.03.2016 tarihli kararı ile hakkında sistemi bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan, 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrası, 53 üncü maddesinin birinci fıkrası ve 58 ... maddesi uyarınca 6 ay hapis cezası ile cezalandırılmasına, hak yoksunluklarına ve tekerrür hükümlerinin uygulanmasına karar verilmiştir.

II. TEMYİZ SEBEPLERİ

Sanığın temyiz isteği, kararın hukuka aykırı olduğuna ilişkin olup, somut bir nedene dayanmamaktadır.

III. OLAY VE OLGULAR

1. Dava konusu olay, sanığın, tanık A. A.'nın sahibi olduğu ... internet cafeye giderek 88.***.**.155 IP nolu adresini kullanmak suretiyle katılan ...'nün e-posta ve facebook adreslerini rızası dışında ele geçirerek kullanılamaz hale getirdiği iddiasına ilişkindir.

2. Antalya İl Emniyet Müdürlüğünün 09.01.2014 tarihli yazısı ile olay günü mağdurun hesaplarına girilen adresin abone tanık A. A.'ın Antalya ili ... ilçesinde bulunan internet kafe adresinden erişim sağlandığı tespit edilmiştir.

3. Tanık A. A., 2006 yılından beri işletmekte olduğu internet kafeye sanığın geldiği dönemde bir çok mağdurun hesaplarını ele geçirerek dolandırmaya çalıştığını, sanığın benzer eylemlerden yargılandığı ve kendisinin de bu dosyalarda tanık veya sanık sıfatı ile ifade verdiğini beyan etmiştir.

4. Sanık, ... aracılığıyla kendisine gelen havaleleri almak için, ... yanında bulunan internet kafeye gittiğini, atılı suçu işlemediğini beyan etmiştir.

5. Mahkeme, tanık A.A, beyanı ve dosya arasına alınan ilam örneklerinden sanık hakkında suç tarihinde birden fazla kişinin facebook ve mail adreslerini ele geçirerek benzer şekilde birçok suç işlediği, aynı mahkemenin 2014/950 Esas sayılı dosyasında sanığın yine farklı bir mağdurun facebook ve mail adreslerini, annesi adına kayıtlı ancak kendisinin kullandığı IP adresinin ait olduğu cep telefonu numarası ile ele geçirdiği gerekçesiyle sanığın atılı suçu işlediğini kabul etmiştir.

IV. GEREKÇE

Tekerrüre esas alınan ilamda yer ... 5237 sayılı Kanun'un 157 nci maddesinin birinci fıkrasında düzenlenen dolandırıcılık suçu, hükümden sonra 02.12.2016 tarihinde yürürlüğe giren 6763 sayılı Kanun'un 34 üncü maddesiyle değişik 5271 sayılı Kanun'un 253 üncü

maddesi ve bu maddeye eklenen fıkraya göre uzlaştırma kapsamına alınmış ise de bu hususun infaz aşamasında gözetilmesi mümkün görülmüştür.

Dosyadaki olay ve olgular karşısında, sanığın savunmasına itibar edilmemiştir. Mahkemenin suçun sübutu ve nitelendirmesinde isabetsizlik görülmemiştir. Yargılama sürecindeki işlemlerin usul ve kanuna uygun olarak yapıldığı, aşamalarda ileri sürülen iddia ve savunmaların toplanan tüm delillerle birlikte gerekçeli kararda tartışıldığı, tanık A.A. tarafından işletilen internet kafeden şikayetçinin bilişim sistemine girmek suretiyle eylemin sanık tarafından gerçekleştirildiği, vicdanî kanının dosya içindeki belge ve bilgilerle uyumlu olarak kesin verilere dayandırıldığı, eyleme uyan suç vasfı ile yaptırımların doğru biçimde belirlendiği anlaşıldığından, sanığın temyiz itirazı yönünden hükümde hukuka aykırılık görülmemiştir.

II.KARAR

Gerekçe bölümünde yer ... nedenlerle Finike Asliye Ceza Mahkemesinin, 15.03.2016 tarihli ve 2015/310 Esas, 2016/330 Karar sayılı kararında sanığın somut bir nedene dayanmayan temyiz itirazları ve dikkate alınan sair hususlar yönünden herhangi bir hukuka aykırılık görülmediğinden sanığın temyiz itirazının reddiyle hükmün, Tebliğnameye uygun olarak, oy birliğiyle ONANMASINA,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 12.01.2023 tarihinde karar verildi.

Kararda TCK m. 244 gereğince yargılama sürecindeki işlemlerin usul ve kanuna uygun olarak yapıldığı, aşamalarda ileri sürülen iddia ve savunmaların toplanan tüm delillerle birlikte gerekçeli kararda tartışıldığı, tanık A.A. tarafından işletilen internet kafeden şikayetçinin bilişim sistemine girmek suretiyle eylemin sanık tarafından gerçekleştirildiği, vicdanî kanının dosya içindeki belge ve bilgilerle uyumlu olarak kesin verilere dayandırıldığı, eyleme uyan suç vasfı ile yaptırımların doğru biçimde belirlendiği anlaşıldığından, sanığın temyiz itirazı yönünden hükümde hukuka aykırılık görülmemekle yerel mahkeme kararının onanmasına karar verilmiştir.

KARAR 17:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2020/11457
Karar No: 2023/117
Karar Tarihi: 18-01-2023

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçu – Temyiz davasına konu dosyalarda lehe hükümler içeren 5271 sayılı kanını uygulanması imkanının doğması ve bu konuda mahkemesince yeniden değerlendirme yapılması gereği- Hükmün bozulması

ÖZET: Maddi ceza hukukuna ilişkin hükümler içeren basit yargılama usulünün \"hükme bağlanmış dosyalarda\" uygulanmasını engelleyen 5271 sayılı Kanunu'nun geçici 5 ... maddesinin (d) bendindeki \"hükme bağlanmış\" ibaresinin basit yargılama usulü yönünden Anayasa Mahkemesi tarafından iptal edilmesi nedeniyle temyiz davasına konu dosyalarda lehe hükümler içeren 5271 sayılı Kanunu'nun 251 ... maddesinin üçüncü fıkrasının uygulanması imkanının doğması ve bu konuda mahkemesince yeniden değerlendirme yapılmasında yasal zorunluluk bulunmaktadır.

(AİHS m. 7) (2709 S. K. m. 38) (5320 S. K. m. 8) (1412 S. K. m. 223, 305, 310, 317) (5271 S. K. m. 260, Geç. m. 5) (5237 S. K. m. 243)

Sanıklar hakkında bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan kurulan hükümlerin; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 ... maddesi gereği yürürlükte bulunan 1412 sayılı Ceza

Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 ... maddesi gereği temyiz edilebilir oldukları, karar tarihinde yürürlükte bulunan 5271 sayılı Kanun'un 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükümleri temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

II. HUKUKÎ SÜREÇ

Sanıklar hakkında bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan açılan davada, Malatya 3. Asliye Ceza Mahkemesinin 24.03.2016 tarihli kararı ile sanıklar hakkında katılan ...'ya karşı bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan, 1412 sayılı Kanun'un 223 üncü maddesinin ikinci fıkrasının (e) bendi uyarınca ayrı ayrı beraatlerine karar verilmiştir.

III. TEMYİZ SEBEPLERİ

Katılanın temyiz isteği; sanıkların suçu ikrar ettikleri, eksik inceleme ve araştırma yapıldığı, delillerin takdirinde hata yapıldığı, kararın yasal dayanağı olmadığına ilişkindir.

III. OLAY VE OLGULAR

1. Dava konusu olay, sanık ... suç tarihinde resmi nikahlı olduğu katılanın kendisini aldattığından şüphelendiği, Malatya ilinde ikamet eden kardeşi sanık ...'yı arayarak, katılanın kullandığı *******9407 nolu GSM hattının online işlemlerine girmesini istemesi üzerine, sanık ...'nın, sanık ...'nın bildirdiği şifre ile katılana ait GSM hattının online işlemlerine rızası olmaksızın internet üzerinden girerek sanık ...'ya katılanın arama kayıtlarını söylediği iddiasına ilişkindir.

2. Avea İletişim Hizmetleri A.Ş.'nin 08.05.2015 tarihli cevap yazısında, katılanın kullandığı telefona ait online işlemeler menüsüne 07.01.2015 tarihinde saat 18.00 sıralarında web erişimi yapan IP numarasının sanık ...'ya ait mobil hat üzerinden sağlandığı tespit edilmiştir.

3. Sanıklar, suç kastı olmaksızın, katılanın GSM hattının online işlemlerine rızası olmaksızın internet üzerinden girdiklerini kabul etmişlerdir.

IV. GEREKÇE

1. Sanık ...'nın, yanında bulunduğu katılanın telefonundan elde ettiği şifreyi kardeşi sanık ...'ya iletmesi üzerine, sanık ...'nın, rızası dışında katılanın GSM hattına ait online işlemlerine girerek görüşme kayıtlarını sanık ...'ya bildirdiği olayda, katılan beyanını doğrular sanıkların tevilli ikrarları ve katılana ait GSM hattının online işlemlerine web erişimi yapan IP nin sanık ...'ya ait mobil hat üzerinden sağlandığı tespiti karşısında, sanıkların atılı suçtan 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 243 üncü maddesinin birinci fıkrası uyarınca cezalandırılmaları yerine yazılı şekilde ayrı ayrı beraatlerine karar verilmesinde hukuka uygunluk bulunmamıştır.

2. Yukarıdaki bozma sebebine bağlı olarak; Dairemizin 2020/2463 Esas sayılı dosyasında 01.10.2020 tarihli kararla, somut norm denetimi yoluyla iptal istemli başvuru üzerine Anayasa Mahkemesinin 14.01.2021 ... ve 2020/81 Esas, 2021/4 sayılı Kararı ile 5271 sayılı Ceza Muhakemesi Kanununa 17.10.2019 tarih ve 7188 sayılı Kanunun 31 ... maddesiyle eklenen geçici 5 ... maddesinin \"01.01.2020 tarihi itibariyle... hükme bağlanmış ve kesinleşmiş dosyalarda .... basit yargılama usulü uygulanmaz\" bölümündeki hükme bağlanmış\" ibaresinin Anayasa'nın 38 ... maddesine aykırı olduğuna ve iptaline karar verilmiştir.

2709 sayılı Türkiye Cumhuriyeti Anayasasının 38 ... maddesinde suçun kanuniliği ve cezanın kanuniliği güvence altına alınmıştır. Avrupa İnsan Hakları Sözleşmesinin 7 nci maddesinin birinci fıkrasında da aynı güvencelere yer verilerek \"lehe kanunun uygulanması ilkesi\" benimsenmiştir.

Maddi ceza hukukuna ilişkin hükümler içeren basit yargılama usulünün \"hükme bağlanmış dosyalarda\" uygulanmasını engelleyen 5271 sayılı Kanunu'nun geçici 5 ... maddesinin (d) bendindeki \"hükme bağlanmış\" ibaresinin basit yargılama usulü yönünden Anayasa Mahkemesi tarafından iptal edilmesi nedeniyle temyiz davasına konu dosyalarda lehe hükümler içeren 5271 sayılı Kanunu'nun 251 ... maddesinin üçüncü fıkrasının uygulanması imkanının doğması ve bu konuda mahkemesince yeniden değerlendirme yapılmasında yasal zorunluluk bulunmaktadır.

II. KARAR

Gerekçe bölümünde açıklanan nedenlerle Malatya 3. Asliye Ceza Mahkemesinin, 24.03.2016 tarihli ve 2015/765 Esas, 2016/346 Karar sayılı kararına yönelik katılanın temyiz

isteği yerinde görüldüğünden hükümlerin, 1412 sayılı Kanun'un 321 ... maddesi gereği, Tebliğname'ye uygun olarak, oy birliğiyle BOZULMASINA,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

18.01.2023 tarihinde karar verildi.

Kararda lehe hüküm içeren maddelerin uygulanması gerektiğinden yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 18:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2020/11515
Karar No: 2021/16487
Karar Tarihi: 22-06-2021

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Sahte banka veya kredi kartının kullanılması suretiyle yarar sağlama suçu – Zincirleme şekilde suçun oluşturduğu gözetilmeden bu suç yönünden mağdur sıfatı bulunmayan işyeri sahiplerine karşı ayrı ayrı hükümler kurulması- Hükmün bozulması

ÖZET: Sanıkların aynı sahte kredi kartını farklı işyerlerinde kullanılması nedeniyle eylemlerinin TCK'nın 245/3, 43. maddelerinde düzenlenen zincirleme şekilde sahte kredi kartının kullanılması suretiyle yarar sağlama suçunu oluşturduğu gözetilmeden bu suç yönünden mağdur sıfatı bulunmayan işyeri sahiplerine karşı ayrı ayrı hükümler kurulması bozmayı gerektirmiştir.

(5237 S. K. m. 43, 243, 245)

Gereği görüşülüp düşünüldü:

Sanıklar ... ve ... hakkında sahte banka veya kredi kartının kullanılması suretiyle yarar sağlama suçundan kurulan mahkumiyet hükümlerine yönelik sanık ... ile sanık ... ve müdafii tarafından yapılan temyiz taleplerinin incelenmesinde;

Başkasına ait banka hesabıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi TCK.nın 245/2. maddesinde; sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise anılan maddenin 3. fıkrasında birbirinden bağımsız ve ayrı ayrı suçları oluşturduğu, bankaya ait gerçek bir kredi kartının manyetik şerit bilgilerinin kopyalanarak sahte bir kredi kartı üretilmesi ve bu kartı kullanmak suretiyle yarar sağlanması halinde suçtan zarar görenin ilgili banka olduğu, kartları gerçeğe aykırı olarak üretilen banka sayısınca TCK.nın 245/2. maddesi ile aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda 43. maddesinin, sahte olarak üretilen kartların alışverişte kullanılması halinde ise, banka sayısınca TCK.nın 245/3. maddesi ile aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise TCK.nın 43. maddesi uyarınca uygulama yapılması gerektiği cihetle

Oluşa ve tüm dosya kapsamına göre; olay tarihinde sanıkların bulunduğu araçta yapılan aramada ele geçirilen 1 adet İnternational Bank'a ait 4999 ... 5030 nolu, 1 adet Citibank'a ait 4652 ..... 9290 nolu, 1 adet Landesbank'a ait 4242 ....5041 nolu, 1 adet First National Banka ait 4901 .... 9020 nolu kredi kartlarının hangisi ya da hangilerinin suça konu olayda kullanıldığının tespit edilemediği, mağdurlara ait işyerinde kontör alımında kullanılan ancak ele geçirilemeyen kredi kartı sliplerinde yer alan Cihan ... adına düzenlenmiş 5200.... 9810 nolu kredi kartının hangi bankaya ait olduğu, sahte olup olmadığının net ve kesin bir biçimde tespit edilmediğinin anlaşılması karşısında; bu kartların kullanılıp kullanılmadığı, kullanıma dair herhangi bir soruşturma veya kovuşturmanın bulunup bulunmadığının araştırılması ve sonucuna göre herbir yabancı banka kartının kullanılması nedeniyle ayrı ayrı TCK'nın 245/3. maddesinin uygulanması gerektiği gözetilmeden eksik araştırmayla yazılı şekilde hükümler kurulması

Kabule göre de;

1-Sanıkların aynı sahte kredi kartını farklı işyerlerinde kullanılması nedeniyle eylemlerinin TCK'nın 245/3, 43. maddelerinde düzenlenen zincirleme şekilde sahte kredi kartının

kullanılması suretiyle yarar sağlama suçunu oluşturduğu gözetilmeden bu suç yönünden mağdur sıfatı bulunmayan işyeri sahiplerine karşı ayrı ayrı hükümler kurulması,
2-Gerekçede ve kısa kararda suçun niteliğinin doğru tespit edilmiş olmasına rağmen uygulama maddesinin TCK.nın 245/3. maddesi yerine TCK.nın 243/3. maddesi olarak yazılması
Yasaya aykırı, sanık ... ile sanık ... ve müdafinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükümlerin bu sebeplerden dolayı 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken CMUK.nın 321. maddesi uyarınca BOZULMASINA, 22.06.2021 gününde oybirliği ile karar verildi.

Kararda aynı sahte kredi kartını farklı işyerlerinde kullanılması nedeniyle eylemlerinin TCK'nın 245/3, 43. maddelerinde düzenlenen zincirleme şekilde sahte kredi kartının kullanılması suretiyle yarar sağlama suçunu oluşturduğu gözetilmeden bu suç yönünden mağdur sıfatı bulunmayan işyeri sahiplerine karşı ayrı ayrı hükümler kurulması gerektiğinden yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 19:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2020/12314
Karar No: 2023/2143
Karar Tarihi: 10-04-2023

Bilişim sisteminin işleyişini engelleme veya bozma suçu- Sanık tarafından muhtelif tarihlerde açılan hesaplarına maaşlarının aktarıldığından dolayı bireysel kredi taksitlerinin gecikmeli olarak tahsil edilmesine neden olduğu - Hükmün bozulması
ÖZET: Sanığın 07.05.2010 tarihinde 6.000,00 TL ve 02.06.2010 tarihinde 15.000,00 TL 'lik bireysel kredi kullandığı, kredi taksitlerinin tahsilatı için 36412069-5002 nolu maaş hesabı tanımlandığı, sanık tarafından muhtelif tarihlerde açılan 36412069-5002 hesabına 15.04.2010-15.10.2010 tarihleri arasındaki maaşlarının, 36412069-5004 nolu hesabına 17.01.2011 maaşının, 36412069-5005 nolu hesabına 15.02.2011-15.03.2011 tarihleri arasındaki maaşlarının, 412069-5007 nolu hesabına 15.04.2011-15.03.2013 tarihlerinde maaşlarının aktarıldığından dolayı bireysel kredi taksitlerinin gecikmeli olarak tahsil edilmesine neden olduğunu ve 36412069-1005 nolu kredi hesabı 13.09.2011 tarihinde 11.976,28-TL'lik bakiyesi tasfiye olunacak alacaklar hesabına aktarıldığı bildirilmiştir. Sanığın iddia edilen yargılama konusu eyleminin 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü maddesinde düzenlenen suçu oluşturduğu, bu suç uyarınca belirlenecek cezanın türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır. 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 03.03.2015 tarihli ilk sorgu tarihi olduğu ve bu tarihten, temyiz incelenmesi tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir.
(5237 S. K. m. 67, 244) (237 S. K. m. 16) (5271 S. K. m. 231) (1412 S. K. m. 305, 310, 317)
Sanık hakkında 237 sayılı Kanun'a aykırılık suçundan 5271 sayılı Ceza Muhakemesi Kanunu'nun (5271 sayılı Kanun) 231 inci maddesinin beşinci fıkrası uyarınca verilen hükmün açıklanmasının geri bırakılması kararının; Yargıtay Ceza Genel Kurulunun, 03.02.2009 tarihli ve 2008/11-250 Esas, 2009/13 Karar sayılı kararı ile 5271 sayılı Kanun'un 231 inci maddesinin onikinci fıkrası gereği itiraz yoluna tabi olduğu, temyizinin mümkün olmadığı anlaşılmıştır.

Sanık hakkında bilişim sisteminin işleyişini engelleme veya bozma suçundan kurulan hükmün; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 inci maddesi gereği temyiz edilebilir olduğu, iddia edilen eylemin 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 244 üncü maddesinin birinci fıkrasında düzenlenen \"bilişim sisteminin işleyişini engelleme veya bozma\" suçuna ilişkin olduğu, bu suçun mağdurunun sistemi kullanılan kişi veya şirket olması nedeniyle atılı suçtan doğrudan zarar gören PTT A.Ş.'nin davaya katılma ve karar tarihinde yürürlükte bulunan 5271 sayılı Kanun'un 260 ıncı maddesinin birinci fıkrası gereği hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmiştir.

İlk derece mahkemesinin katılan PTT A.Ş. vekilinin temyiz talebinin reddine ilişkin 24.11.2015 tarihli ek kararının kaldırılarak yapılan incelemede;

I. HUKUKÎ SÜREÇ

1. Sanık hakkında Uşak Cumhuriyet Başsavcılığının 08.09.2014 tarihli iddianamesi ile 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 244 üncü maddesinin birinci, ikinci fıkrası, 237 sayılı Kanun'un 16 ncı maddesi ve 53 üncü maddesi uyarınca cezalandırılması talebiyle dava açılmıştır.

2. Uşak 5. Asliye Ceza Mahkemesinin, 10.11.2015 tarihli kararı ile sanık hakkında,

a. Bilişim sistemini engelleme veya bozma suçundan 5271 sayılı Kanun'un 223 üncü maddesinin ikinci fıkrasının (e) bendi uyarınca beraat kararı verilmiştir.

b. 237 sayılı Kanun'a aykırılık suçundan 237 sayılı Kanun'un 16 ncı maddesi ve 5237 sayılı Kanun'un 53 üncü maddesi uyarınca 5 ay hapis cezası ile cezalandırılmasına ve sanık hakkında 5271 sayılı Kanun'un 231 inci maddesinin beşinci fıkrası uyarınca verilen hükmün açıklanmasının geri bırakılmasına karar verilmiştir.

II. TEMYİZ SEBEPLERİ

Katılan vekilinin temyiz sebebi; hükmün açıklanmasının geriye bırakılması kararında vekalet ücreti verilmesi gerektiğine, bilişim sistemini engelleme veya bozma suçundan suçun sübut bulduğuna ilişkindir.

III. OLAY VE OLGULAR

1. Dava konusu olay, sanığın, Uşak PTT Başmüdürlüğü İdari ve Mali Birimler Müdürlüğüne ... plakalı aracı özel işlerinde kullanmak suretiyle 237 sayılı Taşıt Kanunu'nun 16 ıncı maddesinde tanımlanan taşıt kanununa muhalefet suçunu işlediği ve Uşak Ziraat Bankasında açtığı banka hesaplarını, maaş tahakkuk programına yetkisiz ve izinsiz olarak girerek maaş hesabını değiştirmek suretiyle her defasında kredi taksidinin ödemesini geciktirmek suretiyle söz konusu işlem bankaca deşifre edilene kadar kendine menfaat sağladığı iddiasına ilişkindir.

2. T.C. Ziraat Bankası Uşak Şubesinin 20.08.2015 tarihli cevabi yazısında; sanığın 07.05.2010 tarihinde 6.000,00 TL ve 02.06.2010 tarihinde 15.000,00 TL 'lik bireysel kredi kullandığı, kredi taksitlerinin tahsilatı için 36412069-5002 nolu maaş hesabı tanımlandığı, sanık tarafından muhtelif tarihlerde açılan 36412069-5002 hesabına 15.04.2010-15.10.2010 tarihleri arasındaki maaşlarının, 36412069-5004 nolu hesabına 17.01.2011 maaşının, 36412069-5005 nolu hesabına 15.02.2011-15.03.2011 tarihleri arasındaki maaşlarının, 412069-5007 nolu hesabına 15.04.2011-15.03.2013 tarihlerinde maaşlarının aktarıldığından dolayı bireysel kredi taksitlerinin gecikmeli olarak tahsil edilmesine neden olduğunu ve 36412069-1005 nolu kredi hesabı 13.09.2011 tarihinde 11.976,28-TL'lik bakiyesi tasfiye olunacak alacaklar hesabına aktarıldığı bildirilmiştir.

3. PTT A.Ş.'nin2.05.2014 tarihli cevabi yazısında; maaş hesap bilgisinin değiştirildiği tarihlerde LOG bilgilerinin tutulmadığı bildirilmiştir.

4. Sanığın sistemde maaşının yatacağı hesap bilgileri dışında bir değişiklik yapılmadığının tespit edildiği bildirilmiştir.

IV. GEREKÇE

A. Sanık Hakkında 237 Sayılı Kanun'a Aykırılık Suçundan Kurulan Hüküm Yönünden;

Sanık hakkında 5271 sayılı Kanun'un 231 inci maddesinin beşinci fıkrası uyarınca verilen hükmün açıklanmasının geri bırakılması kararının; Yargıtay Ceza Genel Kurulunun, 03.02.2009 tarihli ve 2008/11-250 Esas, 2009/13 Karar sayılı kararı ile 5271 sayılı Kanun'un

231 inci maddesinin onikinci fıkrası gereği itiraz yoluna tabi olduğu, temyizinin mümkün olmadığı ve itiraz başvurusunun da merciine değerlendirilmiş olduğu anlaşılmakla incelenmeksizin iadesine karar verilmesi gerektiği anlaşılmıştır.

B. Sanık Hakkında Bilişim Sistemini Engelleme Veya Bozma Suçundan Kurulan Hüküm Yönünden

1.Sanığın iddia edilen yargılama konusu eyleminin 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü maddesinde düzenlenen suçu oluşturduğu, bu suç uyarınca belirlenecek cezanın türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır.

2.5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 03.03.2015 tarihli ilk sorgu tarihi olduğu ve bu tarihten, temyiz incelenmesi tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir.

V. KARAR

A. Sanık Hakkında 237 Sayılı Kanun'a Aykırılık Suçundan Kurulan Hüküm Yönünden;

Gerekçe bölümünde (A) bendinde açıklanan nedenle kanun yolu incelemesinin itiraz merciine yapılması gerektiği ve itiraz merciine de bir karar verildiği anlaşılmakla, dava dosyasının, Tebliğname'ye uygun olarak, oy birliğiyle İNCELENMEKSİZİN İADESİNE,

B. Sanık Hakkında Bilişim Sistemini Engelleme Veya Bozma Suçundan Kurulan Hüküm Yönünden

Gerekçe bölümünde (B) bendinde nedenlerle Uşak 5. Asliye Ceza Mahkemesinin, 10.11.2015 tarihli kararına yönelik katılan vekilinin temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 inci maddesinin birinci fıkrası gereği BOZULMASINA, bu husus yeniden yargılamayı gerektirmediğinden aynı Kanun'un 322 nci maddesinin birinci fıkrasının (1) numaralı bendinin verdiği yetkiye dayanılarak sanık hakkındaki kamu davasının 5271 sayılı Kanun'un 223 üncü maddesinin sekizinci fıkrası gereği gerçekleşen zamanaşımı nedeniyle, Tebliğnameye aykırı olarak, oy birliğiyle DÜŞMESİNE,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 10.04.2023 tarihinde karar verildi.

Kararda yargılama konusu eyleminin 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü maddesinde düzenlenen suçu oluşturduğu, bu suç uyarınca belirlenecek cezanın türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır. 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 03.03.2015 tarihli ilk sorgu tarihi olduğu ve bu tarihten, temyiz incelenmesi tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiş olup, yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 20:

T.C.
YARGITAY
12.Ceza Dairesi
Esas No: 2021/1911
Karar No: 2021/6594
Karar Tarihi: 06-10-2021

Hakaret suçu – Zamanaşımını kesen en son işlem olan suça sürüklenen çocukla birlikte aynı suçları işlediği iddia olunan sanığın sorgu ve savunmasının alındığı tarih olduğu – Beraat kararı verilmesini gerektirir şartlar da bulunmadığı – Davaların düşmesi

ÖZET: Eylemler, TCK'nın 125/2. maddesinde hakaret, TCK'nın 243/1. maddesinde bilişim sistemine girme ve TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal başlığı altında yaptırıma bağlanmış olup, TCK'nın 66/1-e maddesi gereğince anılan suçların asli dava zamanaşımı süresinin 8 yıl olduğu; ancak, 01.08.2012 tarihinde işlendiği iddia edilen eylemlerin işlendiği sırada suça sürüklenen çocuğun onbeş yaşını doldurmuş olup da onsekiz yaşını doldurmamasından dolayı TCK'nın 66/2. maddesi uyarınca 15-18 yaş grubundaki suça sürüklenen çocuk açısından asli dava zamanaşımı süresinin 5 yıl 4 ay olduğu, TCK'nın 67/4. maddesi göz önünde bulundurulduğunda kesen nedenlerin varlığı halinde süre yeniden işlemekte ise de, zamanaşımını kesen en son işlem olan suça sürüklenen çocukla birlikte aynı suçları işlediği iddia olunan sanık ...'ın sorgu ve savunmasının alındığı 19.11.2013 tarihinden itibaren TCK'nın 66/1-e ve 66/2. maddelerinde öngörülen 5 yıl 4 aylık zamanaşımının temyiz inceleme tarihinden önce gerçekleştiği anlaşıldığından, CMK'nın 223/9. maddesindeki derhal beraat kararı verilmesini gerektirir şartlar da bulunmadığından, katılan vekilinin temyiz itirazları bu itibarla yerinde görülmüş olup, sair yönleri incelenmeksizin hükümlerin gerçekleşen zamanaşımı nedeniyle 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince BOZULMASINA; ancak, yeniden yargılama gerektirmeyen bu konuda, suça sürüklenen çocuk hakkındaki davaların ayrı ayrı düşmesine karar verilmiştir. (5271 S. K. m. 223, 231, 264) (5237 S. K. m. 66, 67, 125, 134, 243)

Dava ve Karar: Hakaret ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından sanık ... hakkında verilen hükmün açıklanmasının geri bırakılmasına ilişkin kararlar ile bilişim sistemine girme, tehdit suçlarından sanık ...'ın ve hakaret, bilişim sistemine girme, görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarından suça sürüklenen çocuk ...'in beraatlerine ilişkin hükümler, katılan vekili tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

A) Sanık ... hakkında hakaret ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından verilen hükmün açıklanmasının geri bırakılmasına ilişkin kararlara yönelik temyiz isteminin incelenmesinde;

Hükmün açıklanmasının geri bırakılması kararının, CMK'nın 231/12. maddesi uyarınca itiraz kanun yoluna tabi bulunduğu, aynı Kanun'un 264. maddesi uyarınca kabul edilebilir bir başvuruda mercide yanılmanın başvuranın hakkını ortadan kaldırmayacağı, mahkemece kararın temyize değil, itiraza tabi olduğu belirtilip, katılan vekilinin temyiz isteminin, itiraz mahiyetinde değerlendirilmesi için CMK'nın 264/2. maddesi uyarınca dosyanın merciine gönderildiği ve Denizli 3. Ağır Ceza Mahkemesinin 26.11.2015 tarihli, 2015/950 değişik iş sayılı kararıyla katılan vekilinin itirazının reddine karar verildiği anlaşılmakla; dosyanın incelenmeksizin mahkemesine iadesinin temini için Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

B) Sanık ...'ın bilişim sistemine girme ve tehdit suçlarından beraatine ilişkin hükümlere yönelik temyiz isteminin incelenmesinde;

Sanık ...'ın kız arkadaşı olan suça sürüklenen çocuk ... ile aynı avukatlık bürosunda çalışan mağdur ... arasında uyuşmazlık olduğu dönemde, sanık ...'ın, mağdur ...'e ait facebook hesabı üzerinden, mağdur ...'e yönelik; "...Şunu unutmayın Kader ile çok mutluyuz, onu çok seviyorum, onu üzen her kim olursa olsun ızdırap olurum, sakın bir daha kimse haddi olmayan şeye karışmasın, derdi olan varsa gelsin bana söylesin... umarım mesaj gideceği yere ulaşmıştır" biçiminde mesaj yazmak ve mağdur ...'e ait facebook hesabına giriş yapmak suretiyle bilişim sistemine girme ve tehdit suçlarını işlediğinin iddia edildiği olayda;

Şikayet dilekçesinin kapsamı ve ekindeki internet çıktıları ile dosyada mevcut diğer delillere göre; tehdit suçunu oluşturduğu iddia edilen mesajın, sanık ...'ın kız arkadaşı olan suça sürüklenen çocuk ...'e ait facebook hesabındaki paylaşımın altına sanık ...'ın muhatabı belirsiz şekilde yaptığı yorum niteliğinde olması ve sanık ... mağdur ...'e ait facebook hesabı üzerinden değil, kendisinin açtığı facebook hesapları üzerinden paylaşımda bulunmuş olup, sanık ...'ın mağdur ...'e ait facebook hesabına giriş yapmaması nedeniyle sanık ...'a yüklenen bilişim sistemine girme ve tehdit suçlarının yasal unsurlarının oluşmamasından dolayı sanık ... hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesine ilişkin yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir.

Yapılan yargılama sonunda, yüklenen fiillerin kanunda suç olarak tanımlanmamış olduğu gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılan vekilinin yasal olmayan gerekçelerle görevsiz mahkemece beraat kararı verildiğine, suç vasfına ilişkin temyiz itirazlarının reddiyle, beraate ilişkin hükümlerin isteme uygun olarak ONANMASINA,

C) Suça sürüklenen çocuk ...'in hakaret, bilişim sistemine girme ve görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarından beraatine ilişkin hükümlere yönelik temyiz isteminin incelenmesine gelince;

Suça sürüklenen çocuk ...'e isnat edilen ve daha ağır bir suçu oluşturma ihtimali bulunmayan eylemler, TCK'nın 125/2. maddesinde hakaret, TCK'nın 243/1. maddesinde bilişim sistemine girme ve TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal başlığı altında yaptırıma bağlanmış olup, TCK'nın 66/1-e maddesi gereğince anılan suçların asli dava zamanaşımı süresinin 8 yıl olduğu; ancak, 01.08.2012 tarihinde işlendiği iddia edilen eylemlerin işlendiği sırada suça sürüklenen çocuğun onbeş yaşını doldurmuş olup da onsekiz yaşını doldurmamasından dolayı TCK'nın 66/2. maddesi uyarınca 15-18 yaş grubundaki suça sürüklenen çocuk açısından asli dava zamanaşımı süresinin 5 yıl 4 ay olduğu, TCK'nın 67/4. maddesi göz önünde bulundurulduğunda kesen nedenlerin varlığı halinde süre yeniden işlemekte ise de, zamanaşımını kesen en son işlem olan suça sürüklenen çocukla birlikte aynı suçları işlediği iddia olunan sanık ...'ın sorgu ve savunmasının alındığı 19.11.2013 tarihinden itibaren TCK'nın 66/1-e ve 66/2. maddelerinde öngörülen 5 yıl 4 aylık zamanaşımının temyiz inceleme tarihinden önce gerçekleştiği anlaşıldığından, CMK'nın 223/9. maddesindeki derhal beraat kararı verilmesini gerektirir şartlar da bulunmadığından, katılan vekilinin temyiz itirazları bu itibarla yerinde görülmüş olup, sair yönleri incelenmeksizin hükümlerin gerçekleşen zamanaşımı nedeniyle 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince BOZULMASINA; ancak, yeniden yargılama gerektirmeyen bu konuda, aynı Kanunun 322. maddesi gereğince karar verilmesi mümkün bulunduğundan, aynı maddenin verdiği yetkiye istinaden; suça sürüklenen çocuk hakkındaki davaların TCK'nın 66/1-e, 66/2 ve CMK'nın 223/8. maddeleri gereğince isteme aykırı olarak ayrı ayrı DÜŞMESİNE, 06.10.2021 tarihinde oybirliğiyle karar verildi.

Kararda TCK'nın 243/1. maddesinde bilişim sistemine girme ve TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal başlığı altında yaptırıma bağlanmış olup, TCK'nın 66/1-e maddesi gereğince anılan suçların asli dava zamanaşımı süresinin 8 yıl olduğundan beraat kararı verilmesi gerektiğinden yerel mahkeme kararının bozulmasına karar verilmiştir.

KARAR 21:

T.C.
YARGITAY
8.Ceza Dairesi
Esas No: 2021/6897
Karar No: 2023/147
Karar Tarihi: 19-01-2023

İncelemekte olduğunuz karar https://mevzuat.sinerjias.com.tr adresinden alınmıştır.

Bilişim sistemine hukuka aykırı olarak girme suçu – MEDULA uygulaması dikkate alındığında münhasıran katılanın kullanımına tahsis edilmeyip görevli yetkili personel birimlerce kullanılabildiği - Suçun sanık tarafından işlenmediği – Hükmün onanması

ÖZET: Mevcut deliller karşısında; sanığın bilişim sisteminden sayılan hastaneye ait otomasyan üzerinden katılanın SGK şifresini ele geçirerek giriş yapmadığı, kaldı ki giriş yapıldığı iddia edilen hastaneye ait bilişim sisteminin de MEDULA uygulaması dikkate alındığında münhasıran katılanın kullanımına tahsis edilmeyip hastanede görevli yetkili

personel ve birimlerce de kullanılabildiği anlaşılmakla, atılı suçun sanık tarafından işlenmediği gerekçesiyle verilen beraat kararında isabetsizlik bulunmadığından; katılan vekilinin bilirkişi raporunun ve kararın eksik incelemeye dayandığına, usul ve yasaya aykırı karar verildiğine dair temyiz sebepleri yerinde görülmemiştir.

(5271 S. K. m. 223, 260) (1412 S. K. m. 305, 310, 317) (5237 S. K. m. 43, 53, 244)

Dava ve Karar: Sanık hakkında kurulan hükmün; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 ... maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 ... maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Ceza Muhakemesi Kanunu'nun(5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

1- Sanık hakkında Sakarya Cumhuriyet Başsavcılığı'nın 21.01.2015 tarihli iddianamesi ile bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 244 üncü maddesinin ikinci fıkrası, 43 üncü maddesinin birinci fıkrası, 53 üncü maddesinin birinci fıkrası uyarınca cezalandırılması istemi ile dava açılmıştır.

2- Sakarya 6. Asliye Ceza Mahkemesinin, 02.05.2016 tarihli kararı ile hakkında sistemi bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan, 5271 sayılı Kanun'un 223 üncü maddesinin ikinci fıkrasının b bendi uyarınca beraat kararı verilmiştir.

II. TEMYİZ SEBEPLERİ

Katılan vekilinin temyiz istemleri

1- Bilirkişi raporunun ve verilen kararın eksik incelemeye dayandığına,

2- Usul ve yasaya aykırı karar verildiğine vesaire ilişkindir.

III. OLAY VE OLGULAR

1- Dava konusu olay, katılanın doktor olarak çalıştığı ... ... Hastanesi'nde hizmet sözleşmesinin sonlandırılması üzerine hastane yönetimi aleyhine Sakarya 1. İş Mahkemesi'nde açtığı davada hastane müdürü olan sanığın katılana Sosyal Güvenlik Kurumu tarafından verilen hekim şifresini katılanın bilgisi ve rızası dışında kullanarak daha önceden muayene ettiği 2 hastaya ait özlük dosyasına sistem üzerinden giriş yaptığı ve hastalıklarına ilişkin jinekolojik bulguları içerir epikriz dosyalarını ele geçirerek İş mahkemesinde görülen dava dosyasında kullandığı iddiasına ilişkindir.

2-Sakarya Siber Suçlarla Mücadele Şube Müdürlüğü'nün 23.01.2014 tarihli tutanağı ile olay tarihinde katılana ait sisteme yapılan girişlere dair bilgisayar ve şüpheli şahsın kimliğinin tespit edilemediği belirtilmiştir.

3- Sanık, katılana ait sisteme giriş yapmadığını, katılanın SGK şifresini de bilmesinin mümkün olmadığını belirterek atılı suçlamayı kabul etmemiştir.

4- ... ... Hastanesi çalışanı olan tanıklar V.A, Z.A ve Y.Z; katılana SGK tarafından verilen şifrenin katılan tarafından kendilerine söylenmediği sürece bilmelerinin mümkün olmadığını, katılanın koymuş olduğu teşhis ve yazmış olduğu reçeteyi MEDULA sistemi üzerinden tüm detaylarıyla hastanenin muhasebe birimi, eczaneler ve hastane personelinin tümünün görebildiğini, evrak olarak çıktı alabildiklerini beyan etmişlerdir.

5- Soruşturma aşamasında alınan 22.03.2014 tarihli bilirkişi raporunda, katılanın çalıştığı Sakarya ... ... Hastanesi'ndeki TP Plus hastane otomasyonu, Nucleus hastane otomasyonu, sunucu veritabanının incelenmesi neticesinde oturumu kapatma tarihinin 22.03.2013, saatin ise 20:40.14 olduğu belirlenmiştir.

6- Kovuşturma aşamasında alınan 12.01.2016 tarihli bilirkişi raporunda, katılana kurum web uygulaması üzerinden "SGK Hekim Şifresi" verildiği ve bu şifreyi ancak kendisinin bildiği ve bileceği bir şifre olduğu, katılana ait bilgisayarın katılanın görev yaptığı ve ilişiğinin kesildiği 22.03.2013 tarihine kadar katılan tarafından kullanıldığı ve daha sonra bu sisteme girilmediği, sanığın suça konu eylemi şifreyi bilmediği müddetçe yapmasının mümkün olmadığı belirtilmiştir.

IV. GEREKÇE

1. Sanığın aşamalardaki özünde değişmeyen savunmasının, tanıklar V.A, Z.A ve Y.Z'nin bilgi ve görgüleri, katılan ve sanığın çalıştığı hastaneye ait otomasyon sisteminde katılanın oturum bilgileri üzerinde yapılan teknik incelemeler sonucunda düzenlenen 22.03.2014 ve 12.01.2016 tarihli denetime elverişli bilirkişi raporlarında katılanın sistemine en son girişinin katılanın hastaneden ilişiğinin kesildiği tarihte gerçekleştiği ve katılana ait SGK şifresini bilmeyen sanığın sisteme izinsiz girmesinin mümkün olmadığı yönündeki tespitleriyle doğrulanmıştır.

Mevcut deliller karşısında; sanığın bilişim sisteminden sayılan hastaneye ait otomasyan üzerinden katılanın SGK şifresini ele geçirerek giriş yapmadığı, kaldı ki giriş yapıldığı iddia edilen hastaneye ait bilişim sisteminin de MEDULA uygulaması dikkate alındığında münhasıran katılanın kullanımına tahsis edilmeyip hastanede görevli yetkili personel ve birimlerce de kullanılabildiği anlaşılmakla, atılı suçun sanık tarafından işlenmediği gerekçesiyle verilen beraat kararında isabetsizlik bulunmadığından; katılan vekilinin bilirkişi raporunun ve kararın eksik incelemeye dayandığına, usul ve yasaya aykırı karar verildiğine dair temyiz sebepleri yerinde görülmemiştir.

2- Yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, Mahkemenin yargılama sonuçlarına uygun şekilde oluşan inanç ve takdirine, incelenen dava dosyası içeriğine göre, katılan vekilinin yerinde görülmeyen diğer temyiz sebeplerinin reddine karar verilmesi gerektiği anlaşılmıştır.

V. KARAR

Gerekçe bölümünde açıklanan nedenlerle Sakarya 6. Asliye Ceza Mahkemesinin, 02.05.2016 tarihli ve 2015/92 Esas, 2016/405 Karar sayılı kararında katılan vekili tarafından öne sürülen temyiz sebepleri ve dikkate alınan sair hususlar yönünden herhangi bir hukuka aykırılık görülmediğinden katılan vekilinin temyiz sebeplerinin reddiyle hükmün, Tebliğname'ye uygun olarak, oy birliğiyle ONANMASINA,
Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 19.01.2023 tarihinde karar verildi.

Kararda sanığın bilişim sisteminden sayılan hastaneye ait otomasyan üzerinden katılanın SGK şifresini ele geçirerek giriş yapmadığı, kaldı ki giriş yapıldığı iddia edilen hastaneye ait bilişim sisteminin de MEDULA uygulaması dikkate alındığında münhasıran katılanın kullanımına tahsis edilmeyip hastanede görevli yetkili personel ve birimlerce de kullanılabildiği anlaşılmakla, atılı suçun sanık tarafından işlenmediği gerekçesiyle verilen beraat kararında isabetsizlik bulunmadığından yerel mahkeme kararının onanmasına karar verilmiştir.

KARAR 22:

T.C.
YARGITAY
4.Ceza Dairesi
Esas No: 2021/18163
Karar No: 2023/24635
Karar Tarihi: 23-11-2023

Hakaret suçu – Şikayetçi şüphelilerin geçmişte arkadaş iken daha sonra aralarının bozulduğu – Sanıkların atılı suçları işledikleri – Temyiz sebeplerinin reddiyle hükmün onandığı

ÖZET: Şikâyetçi şüphelilerin geçmişte arkadaş iken daha sonra aralarının bozulduğu, ilerleyen süreçte de birbirlerinin adlarına sahte ... siteleri açtıkları, bu sitelerde ve Whatsapp üzerinden birbirlerine hakaret içerir yazılar yazdıkları, birbirlerinden şikâyetçi oldukları, soruşturma evrakına konu ... ve Whatsapp çıktılarından atılı suçları işledikleri anlaşıldığı

iddiasıyla açılan davada sanıkların atılı suçları işledikleri Yerel Mahkemece kabul olunmuştur. Yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, Mahkemenin yargılama sonuçlarına uygun şekilde oluşan inanç ve takdirine, incelenen dava dosyası içeriğine göre, katılan vekilinin yerinde görülmeyen temyiz sebeplerinin reddine karar verilmesi gerektiği anlaşılmıştır

(5237 S. K. m. 52, 62, 129, 243) (5271 S. K. m. 223) (1412 S. K. m. 305, 310, 317)

Katılan sanık ... müdafiinin 08.04.2016 tarihli süre tutum dilekçesinde, sanık sıfatıyla bilişim sistemine girme suçundan mahkûmiyet hükmünü temyiz ettiği, hakaret suçuna yönelik hakkında verilen ceza verilmesine yer olmadığı kararına dair hiç bir itirazının olmadığı, katılan sıfatıyla sanık ... hakkında hakaret suçundan verilen ceza verilmesine yer olmadığı kararını temyiz ettiği, 07.06.2016 tarihli gerekçeli temyiz dilekçesinde ise hakkında hakaret suçundan verilen ceza verilmesine yer olmadığı kararını da temyiz ettiği ancak temyiz dilekçesinin süresi içinde verilmediği anlaşıldığından, temyiz kapsamının katılan sıfatıyla sanık ... hakkında hakaret suçundan verilen hükme, sanık sıfatıyla bilişim sistemine girme suçundan aleyhine kurulan hükme yönelik olduğu belirlenmiştir.

Sanık ... hakkında bilişim sistemine girme suçundan neticeten hükmolunan 1.500,00 TL adlî para cezasına ilişkin mahkûmiyet kararının, tür ve miktar itibarıyla 5320 sayılı Ceza Muhakemesi Kanunu'nun Yürürlük ve Uygulama Şekli Hakkında Kanun'un (5320 sayılı Kanun) geçici 2 nci maddesi uyarınca kesin nitelikte bulunduğu anlaşılmıştır.

Sanık ..., hakkında hakaret suçundan kurulan hükmün; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 inci maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Kanun'un (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir sebeplerin bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

1. Sanık ... hakkında hakaret suçundan, 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 129 uncu maddesinin üçüncü fıkrası uyarınca ve 5271 sayılı Kanun'un 223 üncü maddesinin dördüncü fıkrasının (c) bendi uyarınca ceza verilmesine yer olmadığı, kararı verilmiştir.

2. Sanık ... hakkında bilişim sistemine girme suçundan, 5237 sayılı Kanun'un 243 üncü maddesinin birinci fıkrası, 62 nci, 52 nci maddeleri uyarınca 1.500,00 TL adli para cezası ile cezalandırılmasına, karar verilmiştir.

3.Sanık .... hakkında hakaret suçundan, 5237 sayılı Kanun'un 129 uncu maddesinin üçüncü fıkrası uyarınca ve 5271 sayılı Kanun'un 223 üncü maddesinin dördüncü fıkrasının (c) bendi uyarınca ceza verilmesine yer olmadığı, kararı verilmiştir.

II. TEMYİZ SEBEPLERİ

Katılan sanık müdafiinin temyiz isteği; kararın usûl ve yasaya aykırı olduğuna, ne şekilde hakaret edildiğinin kararda gösterilmediğine, vesaire ilişkindir.

III. OLAY VE OLGULAR

Şikâyetçi şüphelilerin geçmişte arkadaş iken daha sonra aralarının bozulduğu, ilerleyen süreçte de birbirlerinin adlarına sahte ... siteleri açtıkları, bu sitelerde ve Whatsapp üzerinden birbirlerine hakaret içerir yazılar yazdıkları, birbirlerinden şikâyetçi oldukları, soruşturma evrakına konu ... ve Whatsapp çıktılarından atılı suçları işledikleri anlaşıldığı iddiasıyla açılan davada sanıkların atılı suçları işledikleri Yerel Mahkemece kabul olunmuştur.

IV. GEREKÇE

Sanık ... Hakkında Bilişim Sistemine Girme Suçundan Verilen Hüküm Yönünden

Hükmün tür ve miktarları itibarıyla 14.04.2011 tarihinde yürürlüğe giren

31.03.2011 tarihli ve 6217 sayılı Kanun'un 26 ncı maddesi ile 5320 sayılı Kanun'a eklenen geçici 2 nci maddesi uyarınca kesin nitelikte bulunduğu anlaşılmakla, sanık müdafiinin temyiz isteğinin reddine karar verilmesi gerektiği anlaşılmıştır.

B. Sanık ... Hakkında Hakaret Suçundan Verilen Hüküm Yönünden

Karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Kanun'un 310 uncu maddesinin birinci fıkrasında belirlenen bir haftalık kanunî süre geçtikten sonra temyiz

isteğinde bulunulduğu, hükmün, 1412 sayılı Kanun'un 305 inci maddesinin birinci fıkrası gereği resen temyize de tabi olmadığı anlaşılmakla, sanık müdafiinin temyiz isteğinin, 1412 sayılı Kanun'un 317 nci maddesi uyarınca reddine karar verilmesi gerektiği anlaşılmıştır.

C. Sanık ... Hakkında Hakaret Suçundan Verilen Hüküm Yönünden
1. Katılan Vekilinin Temyiz Sebepleri Yönünden
Tüm dosya kapsamına göre; ... ve ... yazışmalarıyla hakaret eyleminin karşılıklı gerçekleştiği sabit görülerek ceza verilmesine yer olmadığına karar verilmesinde, Mahkemenin inanç ve takdirinde hukuka aykırılık bulunmadığından, katılan vekilinin temyiz sebepleri yerinde görülmemiştir.

2.Sair Hususlar Yönünden
Yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, Mahkemenin yargılama sonuçlarına uygun şekilde oluşan inanç ve takdirine, incelenen dava dosyası içeriğine göre, katılan vekilinin yerinde görülmeyen temyiz sebeplerinin reddine karar verilmesi gerektiği anlaşılmıştır.
V. KARAR
A. Sanık ... Hakkında Hakaret ve Bilişim Sistemine Girme Suçlarından Verilen Hükümlerin Temyizinde
Gerekçe bölümünün (A) ve (B) bentlerinde açıklanan nedenlerle Yerel Mahkemenin kararına yönelik sanık müdafinin temyiz isteğinin, 1412 sayılı Kanun'un 317 nci maddesi gereği, Tebliğname'ye uygun olarak, oy birliğiyle REDDİNE,

B. Sanık ... Hakkında Hakaret Suçundan Verilen Hükmün Temyizinde
Gerekçe bölümünün (C) bendinde açıklanan nedenlerle Yerel Mahkemenin kararında katılan vekili tarafından öne sürülen temyiz sebepleri ve dikkate alınan sair hususlar yönünden herhangi bir hukuka aykırılık görülmediğinden, temyiz sebeplerinin reddiyle hükmün, Tebliğname'ye uygun olarak, oy birliğiyle ONANMASINA,
Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,
23.11.2023 tarihinde karar verildi.

Kararda TCK m. 243 gereğince verilen para cezasının, yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, Mahkemenin yargılama sonuçlarına uygun şekilde oluşan inanç ve takdirine, incelenen dava dosyası içeriğine göre, katılan vekilinin yerinde görülmeyen temyiz sebeplerinin reddine karar verilmiştir.

KARAR 23:

T.C.
YARGITAY
11.Ceza Dairesi
Esas No: 2022/6634
Karar No: 2023/264
Karar Tarihi: 24-01-2023

Dolandırıcılık suçu – Hüküm tarihine kadar sekiz yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu- Herhangi bir hukuka aykırılık görülmediği - Hükmün onanması
ÖZET: Sanıkların yargılama konusu sahtecilik eylemleri için, 5237 sayılı Kanun'un 204 üncü maddesinin birinci fıkrası uyarınca ve sanık ...'in yargılama konusu bilişim sistemindeki verileri değiştirme eylemi için 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü fıkraları uyarınca belirlenecek cezaların türü ve üst haddine göre aynı

Kanun’un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü; 5237 sayılı Kanun’un 67 nci maddesinin ikinci fıkrasının (a) bendi uyarınca zamanaşımı süresini kesen son işlemin 05.03.2013 tarihli sorgu olduğu ve bu tarihten, hüküm tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir. Gerekçe bölümünde açıklanan nedenle ... 1. Ağır Ceza Mahkemesinin, 29.12.2021 tarihli ve 2020/23 Esas, 2021/419 Karar sayılı kararında katılan vekilince öne sürülen temyiz sebepleri ve dikkate alınan sair hususlar yönünden herhangi bir hukuka aykırılık görülmediğinden katılan vekilinin temyiz sebeplerinin reddiyle hükümlerin, Tebliğname’ye uygun olarak, onanmasına karar verilmiştir.

(5271 S. K. m. 223, 260) (1412 S. K. m. 305, 310, 317) (5237 S. K. m. 52, 53, 62, 66, 158, 168, 204, 243, 244)

Sanıklar hakkında kurulan hükümlerin; karar tarihi itibarıyla 6723 sayılı Kanun’un 33 üncü maddesiyle değişik 5320 sayılı Kanun’un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu’nun (1412 sayılı Kanun) 305 inci maddesi gereği temyiz edilebilir olduğu, karar tarihinde yürürlükte bulunan 5271 sayılı Ceza Muhakemesi Kanunu’nun (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükümleri temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun’un 310 uncu maddesi gereği temyiz isteminin süresinde olduğu, aynı Kanun’un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

1. ... 1. Ağır Ceza Mahkemesinin, 24.12.2013 tarihli ve 2013/11 Esas, 2013/429 Karar sayılı kararı ile sanıklar hakkında;

a) Kamu kurum ve kuruluşlarının araç olarak kullanılması suretiyle dolandırıcılık suçundan 5237 sayılı ... Ceza Kanunu’nun (5237 sayılı Kanun) 158 inci maddesinin birinci fıkrasının (d) bendi, 168 inci maddesinin birinci fıkrası, 62 inci, 52 inci, 53 üncü maddeleri uyarınca 6 ... hapis 20 gün ve 20,00 TL adli para cezası ile cezalandırılmalarına ve hak yoksunluklarına,

b) 5237 sayılı Kanun'un 204 üncü maddesinin birinci fıkrası uyarınca yüklenen resmi belgede sahtecilik suçundan beraate,

c) Sanık ... hakkında; 5237 sayılı Kanun'un 244 üncü maddesinin birinci ve üçüncü fıkraları uyarınca yüklenen bilişim sistemini engelleme veya bozma suçundan beraate,

Karar verilmiştir.

2. Yargıtay (Kapatılan) 15. Ceza Dairesinin, 20.11.2019 tarihli ve 2017/8891 Esas, 2019/12369 Karar sayılı kararı ile sanıklar hakkında İlk Derece Mahkemesince kurulan hükümlere yönelik katılan vekili, sanık ... müdafii ve sanık ...'ın temyiz başvurusunun kabulüne karar verilerek sanık ... hakkında nitelikli dolandırıcılık suçundan kurulan hükmün onanmasına; diğer hükümlerin eksik araştırma nedeniyle bozulmasına karar verilmiştir.

3. Bozma üzerine yapılan yargılamada ... 1. Ağır Ceza Mahkemesinin, 29.12.2021 tarihli ve 2020/23 Esas, 2021/419 Karar sayılı kararı ile;

a) Sanık ... hakkında nitelikli dolandırıcılık suçundan hükmün açıklanmasının geri bırakılmasına,

b) Sanıklar hakkında resmi belgede sahtecilik suçundan ve sanık ... hakkında bilişim sistemini engelleme veya bozma suçundan açılan kamu davalarının 5237 sayılı Kanun'un 66 ıncı maddesinin birinci fıkrasının (e) bendi ve 5271 sayılı Kanun'un 223 üncü maddesinin sekizinci fıkrası uyarınca düşmesine,

Karar verilmiştir.

IV. TEMYİZ SEBEPLERİ

Katılan vekilinin temyiz isteği; sanıklar hakkında verilen düşme hükümlerine yönelik olup zamanaşımının dolmadığına ve kararın usûl ve yasaya aykırı olduğuna ilişkindir.

III. GEREKÇE

1. Sosyal Güvenlik Kurumu Rüzgarlı Sosyal Güvenlik Merkezi Tescil ve Genel Sağlık Sigorta Servisinde memur olarak çalışan sanık ... ile aynı kurumun Ulucanlar Sosyal Güvenlik Merkezinde memur olarak görev yapan sanık ...'ın birlikte hareket ederek mağdur ...'ın kuruma olan prim borçlarını kapatmak için mağdurdan 3.000,00 TL aldıkları, sanık ...'in kurumdaki diğer çalışanların şifrelerini kullanarak kurumun sisteminde mağdura ait borcun ödenmiş olarak gösterilmesini sağlayıp aynı kurumda veznedar olarak görev yapan ... ...'a ait

sahte kaşe ve imzalarla tahsilat makbuzları düzenleyerek mağdura verdiklerinin iddia edildiği olayda;

a) Dosya kapsamından suça konu belgelerin sanıkların görevi gereği düzenlemeye yetkili oldukları belgelerden olmadığı anlaşılmakla, Mahkemenin eylemin TCK'nın 204 üncü maddesinin birinci fıkrasına temas ettiği yönündeki kabûlünde isabetsizlik bulunmamıştır.

b) Her ne kadar, Mahkemece sanık ...'in kurumdaki diğer çalışanların şifrelerini kullanarak kurumun sisteminde mağdura ait borcun ödenmiş olarak gösterilmesini sağlama eyleminin TCK'nın 243 üncü maddesinin üçüncü fıkrasında düzenlenen suçu oluşturacağı kabul edilmişse de; sanığın salt bilişim sistemine girme kastıyla hareket etmeyip kastının en başından beri mağdurun sistemde kayıtlı olan borç bilgilerini değiştirmek olduğu anlaşılmakla, eyleminin TCK'nın 244 üncü maddesinin ikinci ve üçüncü fıkralarına temas ettiği anlaşılmıştır.

2. Sanıkların sorgularının 05.03.2013 tarihinde yapıldığı tespit edilmiştir.

3. Sanıkların yargılama konusu sahtecilik eylemleri için, 5237 sayılı Kanun'un 204 üncü maddesinin birinci fıkrası uyarınca ve sanık ...'in yargılama konusu bilişim sistemindeki verileri değiştirme eylemi için 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü fıkraları uyarınca belirlenecek cezaların türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü; 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (a) bendi uyarınca zamanaşımı süresini kesen son işlemin 05.03.2013 tarihli sorgu olduğu ve bu tarihten, hüküm tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir.

4. Gerekçenin (1-b) paragrafında ulaşılan sonuç ile Mahkemenin kabulü arasındaki farkın sonuca etkili olmadığı görülmüştür.

V. KARAR

Gerekçe bölümünde açıklanan nedenle ... 1. Ağır Ceza Mahkemesinin, 29.12.2021 tarihli ve 2020/23 Esas, 2021/419 Karar sayılı kararında katılan vekilince öne sürülen temyiz sebepleri ve dikkate alınan sair hususlar yönünden herhangi bir hukuka aykırılık görülmediğinden katılan vekilinin temyiz sebeplerinin reddiyle hükümlerin, Tebliğname'ye uygun olarak, oy birliğiyle ONANMASINA,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

24.01.2023 tarihinde karar verildi.

Kararda 5237 sayılı Kanun'un 244 üncü maddesinin ikinci ve üçüncü fıkraları uyarınca belirlenecek cezaların türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü ve zamanaşımı süresi gerçekleşmiş olduğundan yerel mahkeme kararının onanmasına karar verilmiştir.

KARAR 24:

T.C.
YARGITAY
11.Ceza Dairesi
Esas No: 2023/3092
Karar No: 2023/6122
Karar Tarihi: 14-09-2023

Bilişim sistemindeki verileri erişilemez kılma suçu - Sekiz yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu – Zamanaşımı süresini kesen son işlemin mahkumiyet kararı verildiği tarih olduğu – Hükmün düzeltilerek onanması

ÖZET: Sanığın yargılama konusu eylemi için, 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrası uyarınca belirlenecek cezanın türü ve üst haddine göre aynı

Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır. 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 17.03.2015 tarihli mahkûmiyet kararı olduğu ve bu tarihten, temyiz inceleme tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir. Gerekçe bölümünde (A) bendinin (3) numaralı fıkrasında açıklanan nedenle Elmalı Ağır Ceza Mahkemesinin, 17.03.2015 tarihli ve 2014/212 Esas, 2015/61 Karar sayılı kararına yönelik sanığın temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 inci maddesi gereği bozulması bu husus yeniden yargılamayı gerektirmediğinden hükmün düzeltilerek onanmasına karar verilmiştir.

(5271 S. K. m. 260) (1412 S. K. m. 305, 310, 317) (5237 S. K. m. 52, 53, 58, 62, 66, 67, 158, 244)

Dava ve Karar: Sanık hakkında kurulan hükümlerin; karar tarihi itibarıyla 6723 sayılı Kanun'un 33 üncü maddesiyle değişik 5320 sayılı Kanun'un 8 inci maddesi gereği yürürlükte bulunan 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (1412 sayılı Kanun) 305 inci maddesi gereği temyiz edilebilir oldukları, karar tarihinde yürürlükte bulunan 5271 sayılı Kanun'un (5271 sayılı Kanun) 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükümleri temyize hak ve yetkisinin bulunduğu, 1412 sayılı Kanun'un 310 uncu maddesi gereği temyiz isteğinin süresinde olduğu, aynı Kanun'un 317 nci maddesi gereği temyiz isteğinin reddini gerektirir bir durumun bulunmadığı yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

Elmalı Ağır Ceza Mahkemesinin, 17.03.2015 Tarihli ve 2014/212 Esas, 2015/61 Karar Sayılı Kararı ile Sanık Hakkında:

1. Nitelikli dolandırıcılık suçundan, 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 158 inci maddesinin birinci fıkrasının (f) bendi, 62 nci, 52 nci , 58 inci ve 53 üncü maddeleri uyarınca 2 yıl 6 ay hapis ve 220,00 TL adli para cezası ile cezalandırılmasına, hak yoksunluklarına ve tekerrür hükümlerinin uygulanmasına,

2. Bilişim sistemindeki verileri erişilmez kılma suçundan, 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrası, 62 nci, 58 inci, 53 üncü maddeleri uyarınca 5 ay hapis cezası ile cezalandırılmasına, hak yoksunluklarına ve tekerrür hükümlerinin uygulanmasına,

Karar verilmiştir.

II. TEMYİZ SEBEPLERİ

Sanığın temyiz dilekçesinde herhangi bir temyiz sebebine yer verilmediği anlaşılmıştır.

III. OLAY VE OLGULAR

Sanığın suç tarihinde katılan ...'ye ait facebook hesabının şifresini kırıp katılan ...'ın arkadaşı olan diğer katılan ...'den para isteyerek bildirmiş olduğu telefon numarasına mobil bankacılık kanalıyla 140,00 TL havale edilmesini sağladığı, havale tutarının aynı gün sanık tarafından A.T.M.'den çekildiği, sanığın eylemi nedeniyle katılan ...'ın facebook hesabına giremediği iddia ve kabul edilmiştir.

IV. GEREKÇE

A. Nitelikli Dolandırıcılık Suçundan Kurulan Hüküm Yönünden

1. Yargılama sürecindeki işlemlerin usûl ve kanuna uygun olarak yapıldığı, aşamalarda ileri sürülen iddia ve savunmaların toplanan tüm delillerle birlikte gerekçeli kararda gösterilip tartışıldığı, eylemin sanık tarafından gerçekleştirildiğinin saptandığı, vicdanî kanının dosya içindeki belge ve bilgilerle uyumlu olarak kesin verilere dayandırıldığı, eyleme uyan suç vasfı ile yaptırımların doğru biçimde belirlendiği anlaşıldığından sanığın yerinde görülmeyen diğer temyiz sebepleri reddedilmiştir.

2. Gerekçeli karar başlığında yanlış gösterilen suç tarihinin Mahkemece \"29.11.2012\" olarak düzeltilmesi; 5237 sayılı Kanun'un 53 üncü maddesinin uygulanmasına ilişkin Anayasa Mahkemesinin 08.10.2015 tarihli ve 2014/140 Esas, 2015/85 Karar sayılı iptal kararının infaz aşamasında gözetilmesi mümkün görülmüştür.

3. Sanık hakkında kurulan hükümde, Yargıtay tarafından düzeltilmesi mümkün olan ve aşağıda gösterilen bozma nedeni dışında bir hukuka aykırılık görülmemiştir.

5237 sayılı Kanun'un 58 inci maddesinin altıncı fıkrası gereğince tekerrür uygulamasına esas alınan Seydişehir Ağır Ceza Mahkemesinin, 23.05.2012 tarihli ve 2011/99 Esas, 2012/77 Karar sayılı ilamının 18.02.2016 tarihinde kesinleşmiş olması

nedeniyle tekerrüre esas alınamayacağı gözetilmeden tekerrür hükümlerinin uygulanmasına karar verilmesi isabetli bulunmamıştır.

B. Bilişim Sistemindeki Verileri Erişilmez Kılma Suçundan Kurulan Hüküm Yönünden

1. Sanığın yargılama konusu eylemi için, 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrası uyarınca belirlenecek cezanın türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır.

2. 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 17.03.2015 tarihli mahkûmiyet kararı olduğu ve bu tarihten, temyiz inceleme tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmiştir.

V. KARAR

A. Nitelikli Dolandırıcılık Suçundan Kurulan Hüküm Yönünden

Gerekçe bölümünde (A) bendinin (3) numaralı fıkrasında açıklanan nedenle Elmalı Ağır Ceza Mahkemesinin, 17.03.2015 tarihli ve 2014/212 Esas, 2015/61 Karar sayılı kararına yönelik sanığın temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 inci maddesi gereği BOZULMASINA, bu husus yeniden yargılamayı gerektirmediğinden aynı Kanun'un 322 nci maddesi gereği hüküm fıkrasından 5237 sayılı Kanun'un 58 inci maddesinin altıncı ve yedinci fıkralarının uygulanmasına ilişkin bölümün tamamen çıkartılması suretiyle hükmün, Tebliğname'ye aykırı olarak, oy birliğiyle DÜZELTİLEREK ONANMASINA,

Gerekçe bölümünde (B) bendinde açıklanan nedenle Elmalı Ağır Ceza Mahkemesinin, 17.03.2015 tarihli ve 2014/212 Esas, 2015/61 Karar sayılı kararına yönelik sanığın temyiz isteği yerinde görüldüğünden hükmün, 1412 sayılı Kanun'un 321 inci maddesinin birinci fıkrası gereği BOZULMASINA, bu husus yeniden yargılamayı gerektirmediğinden aynı Kanun'un 322 nci maddesinin birinci fıkrasının (1) numaralı bendinin verdiği yetkiye dayanılarak sanık hakkındaki kamu davasının 5271 sayılı Kanun'un 223 üncü maddesinin sekizinci fıkrası gereği gerçekleşen zamanaşımı nedeniyle, Tebliğname'ye aykırı olarak, oy birliğiyle DÜŞMESİNE,

Dava dosyasının, Mahkemesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

14.09.2023 tarihinde karar verildi.

Kararda 5237 sayılı Kanun'un 244 üncü maddesinin ikinci fıkrası uyarınca belirlenecek cezanın türü ve üst haddine göre aynı Kanun'un 66 ncı maddesinin birinci fıkrasının (e) bendi gereği 8 yıllık olağan zamanaşımı süresinin öngörüldüğü anlaşılmıştır. 5237 sayılı Kanun'un 67 nci maddesinin ikinci fıkrasının (d) bendi uyarınca zamanaşımı süresini kesen son işlemin 17.03.2015 tarihli mahkûmiyet kararı olduğu ve bu tarihten, temyiz inceleme tarihine kadar, 8 yıllık olağan zamanaşımı süresinin gerçekleşmiş olduğu belirlenmesi nedeniyle yerel mahkeme hükmünün düzeltilerek onanmasına karar verilmiştir.

KARAR 25:

T.C.
YARGITAY
3.Ceza Dairesi
Esas No: 2023/15137
Karar No: 2024/989
Karar Tarihi: 24-01-2024

Bilişim sistemindeki verileri bozma yok etme suçu – Mahkumiyet kararı verilmiş olmakla suç işlemek amacıyla kurulan örgüte üye olma suçundan verilen beraat kararı nedeniyle vekalet ücretine hükmedilmemesinde yasaya aykırılık görülmediği- Hükmün onandığı

ÖZET: Sanık hakkında yargılandığı aynı davada bilişim sistemindeki verileri, bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan mahkumiyet kararı verilmiş olması karşısında, sanık müdafii tarafından sunulan avukatlık hizmetinin bölünmesi mümkün olmadığından, suç işlemek amacıyla kurulan örgüte üye olma suçundan verilen beraat kararı nedeniyle vekalet ücretine hükmedilmemesinde yasaya aykırılık görülmemiş, Bölge Adliye Mahkemesi kararı vekalet ücreti yönünden hukuka uygun bulunmuştur.

(5237 S. K. m. 43, 53, 220, 244) (5271 S. K. m. 286, 298)

İlk Derece Mahkemesince sanık hakkında bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan hükmolunan cezanın tür ve miktarı ile istinaf incelemesi üzerine Bölge Adliye Mahkemesince verilen esastan ret kararı dikkate alındığında, 5271 sayılı Ceza Muhakemesi Kanunu'nun (5271 sayılı Kanun) 286 ncı maddesinin ikinci fıkrasının (a) bendi uyarınca hükmün temyizinin mümkün olmadığı belirlenmiştir.

İlk Derece Mahkemesince sanık hakkında, suç işlemek amacıyla kurulan örgüte üye olma suçundan verilen hükme yönelik istinaf incelemesi üzerine Bölge Adliye Mahkemesi tarafından verilen kararın; 5271 sayılı Kanun'un 286 ncı maddesinin birinci fıkrası uyarınca temyiz edilebilir olduğu, 260 ıncı maddesinin birinci fıkrası gereği temyiz edenin hükmü temyize hak ve yetkisinin bulunduğu, 291 inci maddesinin birinci fıkrası gereği temyiz isteminin süresinde olduğu, 294 üncü maddesinin birinci fıkrası gereği temyiz dilekçesinde temyiz sebeplerine yer verildiği, 298 inci maddesinin birinci fıkrası gereği temyiz isteminin reddini gerektirir sebeplerin bulunmadığı ve sanık müdafiinin temyizinin vekalet ücretine yönelik olduğu yapılan ön inceleme neticesinde tespit edilmekle, gereği düşünüldü:

I. HUKUKÎ SÜREÇ

A. İlk Derece Mahkemesince Sanık Hakkında

1. Bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan, 5237 sayılı Türk Ceza Kanunu'nun (5237 sayılı Kanun) 244 üncü maddesinin ikinci fıkrası, 43 ve 53 üncü maddeleri uyarınca 9 ay hapis cezası ile cezalandırılmalarına ve hak yoksunluklarına,

2. Suç işlemek amacıyla kurulan örgüte üye olma suçundan, 5237 sayılı Kanun'un 220 nci maddesinin birinci fıkrası ve 53 üncü maddesi uyarınca 1 yıl hapis cezasıyla cezalandırılmasına ve hak yoksunluklarına,

Karar verilmiştir.

C. Bölge Adliye Mahkemesince Sanık Hakkında

1.Bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan İlk Derece Mahkemesince kurulan hükme yönelik sanık müdafiinin istinaf başvurusunun esastan reddine, kesin olarak karar verilmiştir.

2. Suç işlemek amacıyla kurulan örgüte üye olma suçundan İlk Derece Mahkemesince verilen hükme mahkûmiyet hükmü kaldırılıp, hukuka aykırılığın düzeltilmesi suretiyle beraat hükmü kurulmuştur.

II. TEMYİZ SEBEPLERİ

Sanık müdafiinin temyiz istemi, sanık lehine vekalet ücretine hükmolunmasına ve sair hukuka aykırılıkların dikkate alınması gerektiğine ilişkindir.

III. GEREKÇE

A. Bilişim Sistemindeki Verileri Bozma, Yok Etme, Erişilmez Kılma ve Sisteme Veri Yerleştirme Suçundan Kurulan Hüküm Yönünden

İlk Derece Mahkemesince hükmolunan cezanın tür ve miktarı ile istinaf incelemesi üzerine Bölge Adliye Mahkemesince verilen esastan ret kararı nazara alınarak, 5271 sayılı Kanun'un 286 ncı maddesinin ikinci fıkrasının (a) bendinde yer verilen; "İlk derece mahkemelerinden verilen beş yıl veya daha az hapis cezaları ile miktarı ne olursa olsun adlî para cezalarına ilişkin istinaf başvurusunun esastan reddine dair bölge adliye mahkemesi kararları" nın temyiz incelemesine tabi olmadığına ilişkin düzenleme ile incelemeye konu suçun, 5271 sayılı Kanun'un 286 ncı maddesinin üçüncü fıkrası kapsamında da bulunmadığı dikkate alındığında, sanık müdafiinin temyiz isteminin, aynı Kanun'un 298 inci maddesinin birinci fıkrası uyarınca reddine karar verilmesi gerektiği belirlenmiştir.

B. Suç İşlemek Amacıyla Kurulan Örgüte Üye Olma Suçundan Verilen Hüküm Yönünden

Sanık hakkında yargılandığı aynı davada bilişim sistemindeki verileri, bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan mahkumiyet kararı verilmiş olması karşısında, sanık müdafii tarafından sunulan avukatlık hizmetinin bölünmesi mümkün olmadığından, suç işlemek amacıyla kurulan örgüte üye olma suçundan verilen beraat kararı nedeniyle vekalet ücretine hükmedilmemesinde yasaya aykırılık görülmemiş, Bölge Adliye Mahkemesi kararı vekalet ücreti yönünden hukuka uygun bulunmuştur.

IV. KARAR

A. Bilişim Sistemindeki Verileri Bozma, Yok Etme, Erişilmez Kılma ve Sisteme Veri Yerleştirme Suçundan Kurulan Hüküm Yönünden

Gerekçe bölümünün (A) bendinde açıklanan nedenle sanık müdafiinin temyiz isteminin, 5271 sayılı Kanun'un 298 inci maddesinin birinci fıkrası uyarınca, Tebliğname'ye uygun olarak, oy birliğiyle REDDİNE,

B. Suç İşlemek Amacıyla Kurulan Örgüte Üye Olma Suçundan Verilen Hüküm Yönünden

Gerekçe bölümünün (B) bendinde açıklanan nedenle Bölge Adliye Mahkemesi kararında sanık müdafii tarafından öne sürülen temyiz sebepleri ve 5271 sayılı Kanun'un 289 uncu maddesinin birinci fıkrası ile sınırlı olarak yapılan temyiz incelemesi sonucunda hukuka aykırılık görülmediğinden, 5271 sayılı Kanun'un 302 nci maddesinin birinci fıkrası gereği, Tebliğname'ye uygun olarak, oy birliğiyle TEMYİZ İSTEMİNİN ESASTAN REDDİ İLE HÜKMÜN ONANMASINA,

Dava dosyasının, 5271 sayılı Kanunun 304 üncü maddesinin birinci fıkrası uyarınca İstanbul 24. Asliye Ceza Mahkemesine, Yargıtay ilâmının bir örneğinin ise İstanbul Bölge Adliye Mahkemesi 26. Ceza Dairesine gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

Kararda TCK m. 244 gereğince davada bilişim sistemindeki verileri, bozma, yok etme, erişilmez kılma ve sisteme veri yerleştirme suçundan mahkumiyet kararı verilmiş olması karşısında, suç işlemek amacıyla kurulan örgüte üye olma suçundan verilen beraat kararı nedeniyle vekalet ücretine hükmedilmemesinde yasaya aykırılık görülmemiş, Temyiz isteminin reddine karar verilmiştir.

4.3. Kişisel Verilerin Korunması ve Veri Güvenliği ile İlgili Yargı Kararları

KARAR 1:

KIŞISEL VERILERI KORUMA KURUMU

Kişinin kişisel verilerinin yer aldığı ihtarnamenin bordrolama hizmeti sunan veri sorumlusu tarafından başka çalışanlara da göndermesi

(6698 S. K. m. 5, 12, 18) (1512 S. K. m. 89, 90)

Karar Tarihi: 07/04/2022

Karar No: 2022/328

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Kuruma intikal eden şikâyette özetle; ilgili kişinin ücretsiz izne gönderildiğine dair veri sorumlusu tarafından kendisine bir ihtarname iletildiği, söz konusu ihtarnamenin yedi kişiye daha gönderildiği, ihtarnamede T.C. kimlik numarası ve adresinin bulunması nedeniyle ilgili kişinin kişisel verilerinin alenen ifşa edildiği belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

İlgili kişinin esasen aynı grup şirketine ait başka bir şirketin çalışanı olduğu ve aynı grup şirketi çatısı altında yer almaları nedeniyle taraflarınca, söz konusu şirket çalışanlarının ücretleri ve çalışma süreleri kapsamında bordrolama hizmeti temin edildiği ve çalışanlara

yönelik bordro oluşturma ve izin kullanım süreçlerinin denetlenerek bunların kontrol ve takip edilmesi hizmeti sunulduğu,

COVID-19 pandemisinden dolayı alınan tedbirler kapsamında ücretsiz izin kullanımının iş yerinde zorunlu hale gelmesi nedeniyle istihdamın sonlanmaması ve iş yeri ile personel sağlığının tehlikeye düşmemesi adına, ilgili kişinin, asıl işvereni olan şirket tarafından ücretsiz izne çıkarıldığı ve bu kapsamda ilgili kişinin ad ve soyadı, T.C. kimlik numarası, adres bilgisi ve pandemi nedeniyle ücretsiz izin uygulanmasına dair bilgilerinin ilgili kişinin işvereni olan şirket tarafından kendilerine aktarıldığı,

İlgili kişi ücretsiz izindeyken, izin süresinin uzatılması kararının kendisine ve onun gibi izinde olan diğer işçilere bildirilmesi için kendilerine telefonla ulaşılmaya çalışıldığı, ancak bu yolla ulaşılamayan işçilerin hem iş yerine gelmelerinde sağlık açısından sakınca bulunması hem de taraflarınca grup şirketlerine sunulan personel izin takip hizmetleri dolayısıyla çalışana noter vasıtasıyla bildirim yapılmasının uygun olacağı düşüncesi ile taraflarının avukatına çalışanın ad ve soyadı, T.C. kimlik numarası, adres ve ücretsiz izin durumuna ilişkin bilgiler gönderilerek ücretsiz izin süresinin uzatıldığının ihtar edilmesinin istendiği,

Bildirim yapılacak personel sayısının fazla olması sebebiyle, usul ekonomisi ve noterlikteki işlemlerin en uygun şekilde gerçekleştirilmesi adına avukatları tarafından vekâleten ihtarname düzenlenerek gönderildiği, noterlik nezdinde yapılan işlemlerde, sair bilgilerin ilgili noterliğe sağlanmasının Noterlik Kanunu ve ikincil mevzuattan kaynaklandığı, ihtarname keşide edilebilmesi için keşidecinin ve muhatabın/muhatapların ad ve soyadı ile T.C. kimlik numaralarının noterliğe sunulmasının, tebligatın sağlıklı yapılabilmesi için yine mevzuat gereğince zorunlu olduğu, bu nedenle birden çok muhatabın yer aldığı ihtarname içerisinde muhatapların bilgilerine yer verildiği ve ilgili kişisel verilerin noterlik ile paylaşıldığı,

Yapılan bu işlemin meşru ve açık bir amaca dayalı olduğu, işleme amacı olan ücretsiz izin süresinin takibi ve çalışana bildirim yapılabilmesi amacı ile sınırlı olarak bahse konu verilerin işlendiği, aktarıldığı ve işlendikleri amaçla bağlantılı olmayan bir şekilde kullanılmadığı, veri işleme faaliyetinin ölçülü olduğu ve kişisel verilerin ihtarname keşide edilmesi için noterlik ile paylaşılmasının ilgili kişinin lehine ve izin durumunun bildirilmesine yönelik olduğu,

İlgili kişiye ait kişisel verilerin, bordrolama destek hizmetleri çerçevesinde ilgili kişinin işvereni olan şirket tarafından kendilerine aktarıldığı ve bu aktarımın hukuki dayanağının 6698 sayılı Kişisel Verilerin Korunması Kanun'unun (Kanun) 5'inci maddesinin (2) numaralı fıkrasının (f) bendi olduğu ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/328 sayılı Kararı ile;

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; "a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkelerine uygun olarak işlenebileceği,

Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı,

Diğer yandan 1512 sayılı Noterlik Kanunu'nun "Düzenleme Şeklinde Yapılması Zorunlu İşlemler" başlıklı 89'uncu maddesinde; "Niteliği bakımından tapuda işlem yapılmasını gerektiren sözleşme ve vekaletnamelerle, vasiyetname, mülkiyeti muhafaza kaydı ile satış, gayrimenkul satış va'di, vakıf senedi, evlenme mukavelesi, evlat edinme ve tanıma, mirasın taksimi sözleşmesi ve diğer kanunlarda öngörülen sair işlemler bu fasıl hükümlerine göre düzenlenir." hükmünün yer aldığı ve yine anılan Kanun'un "Onaylama" başlıklı üçüncü bölümünün "Şekil" başlığını taşıyan 90'ıncı maddesinin; "Hukuki işlemlerin altındaki imzanın onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır. İmzası onaylanan iş kağıdının aslı ilgilisine verilir ve imzalı bir örneği dairede saklanır. Bu örnek harca tabi değildir." hükmünü haiz olduğu,

Somut olayda, veri sorumlusu tarafından ilgili kişinin ve diğer yedi çalışanın bilgilerine aynı ihtarnamede yer verildiğinin görüldüğü ve veri sorumlusu tarafından da bu durumun ikrar edildiği,

Senetler düzenleme ve onaylama şeklinde hazırlanabilmekle birlikte söz konusu belgenin noterlik tarafından "onaylama" şeklinde gerçekleştirildiğinin görüldüğü ve ilgili kişinin kişisel verilerine ek olarak yedi çalışanın da kişisel verilerinin toplu bir şekilde aynı ihtarnamede yer almasından dolayı her birinin kişisel verilerinin birbirleriyle paylaşıldığının anlaşıldığı,

İlgili kişinin ve diğer yedi çalışanın kimlik ve iletişim verisinin ihtarnamede yer alması suretiyle ilgili noterlikle paylaşılması Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" işleme şartı kapsamında yer almakla birlikte söz konusu çalışanların kimlik ve iletişim verisinin aynı ihtarnamede yer alması ve söz konusu ihtarname keşide edilirken herhangi bir şekilde karartma, muhataplara ayrı ayrı keşide etme vb. gibi bir işlem yapılmaması sebebiyle ilgili kişinin kişisel verilerinin diğer çalışanlarla paylaşıldığı ve bu suretle gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmadığı değerlendirmelerinden hareketle;

İlgili kişinin kişisel verilerinin yer aldığı ihtarnamenin veri sorumlusu tarafından yedi kişiye daha gönderildiği iddiasına ilişkin olarak; diğer yedi çalışanla birlikte ilgili kişinin kimlik ve iletişim verisinin aynı ihtarnamede yer alması ve söz konusu ihtarname keşide edilirken de herhangi bir şekilde karartma, muhataplara ayrı ayrı keşide etme vb. işlemin yapılmaması nedeniyle ilgili kişinin kişisel verilerinin diğer çalışanlarla paylaşıldığı, bu çerçevede Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 12'nci maddesinin (1) numaralı fıkrası hükmüne aykırı olduğu değerlendirildiğinden veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına,

Diğer taraftan Karar hakkında Türkiye Noterler Birliğine bilgi verilmesine karar verilmiştir.

KARAR 2:

KIŞISEL VERILERI KORUMA KURUMU

Veri sorumlusu bir E -ticaret sitesinden alışveriş yapan üçüncü kişiye ait sipariş bilgilerinin ilgili kişinin E-posta adresine gönderilmesi

(6698 S. K. m. 3, 4, 5, 12, 18)

Karar Tarihi: 03/08/2022

Karar No: 2022/774

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Kuruma intikal eden şikayette özetle; ilgili kişinin e-posta adresine bir e-ticaret sitesinden alışveriş yapan üçüncü bir kişinin sipariş bilgilerinin gönderildiği, söz konusu e-

posta içeriğinde ödenen tutar, resimli olarak siparişin içeriği, gönderici adı soyadı, alıcının adı soyadı, adresi, telefon numarası gibi bilgilerin açık bir biçimde yer aldığı, ayrıca e-postada yer alan "Sipariş Takibi ve Güncelleme" adlı buton sayesinde tüm sipariş detaylarının görülebileceği bir sayfaya yönlendirme yapıldığı, bu sayfada ise gönderici ve alıcı bilgilerine ek olarak sipariş edilen ürünün içerik adı, ürün kodu, rengi ve gönderici tarafından alıcıyı muhatap gönderi notunun görüntülendiği, gönderici veya alıcı bilgileri ile gönderi notu bilgilerinin düzenlenebilir durumda olmakla birlikte sipariş iptal butonunun da aktif olduğu, söz konusu olayların veri ihlali olduğunu tespit ederek ve şahsına ait kişisel verilerinin de belirttiği şekilde başkaları tarafından görülebileceğini düşünerek öncelikle e-ticaret sitesine ait müşteri hizmetleriyle canlı destek sistemi üzerinden irtibata geçtiği, müşteri hizmetleri tarafından müşterinin isim benzerliği neticesinde yanlış e-posta verdiğinin, bu sebeple söz konusu sipariş bildiriminin iletildiğinin, bu siparişten kendisine ait e-posta adresinin silindiğinin ve artık kendisine bildirim iletilmeyeceğinin ifade edildiği, ancak bahse konu e-posta adresine halen veri sorumlusu e-ticaret sitesi tarafından reklam içerikli e-postaların iletildiği, konunun hata olarak nitelendirilmesinin kişisel verilerin ihlali gerçeğini değiştirmediği, bu itibarla veri ihlalini önlemek adına güvenlik tedbirlerinin alınması konusunda tüm iletişim kanalları üzerinden veri sorumlusuna bilgilendirmede bulunmasına karşın kendisine herhangi bir dönüş yapılmadığı belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

İlgili kişinin konu hakkında kendilerine başvurduğu ve başvuruya ilişkin cevabın ilgili kişinin ikamet adresine gönderildiği,

İlgili kişinin 20.10.2014 tarihinde şikayete konu edilenden farklı bir e-posta ile söz konusu e-ticaret sitesine üyelik oluşturduğu, e-ticaret sitesine kayıtlı tüm üyelerin bilgilerinde yapılan araştırmalar neticesinde şikayete konu siparişte kullanılan e-posta adresi için bir üyelik hesabının bulunmadığı,

Söz konusu siparişin, bir başka kullanıcı tarafından isim benzerliğinden kaynaklı olarak sehven ilgili kişiye ait e-posta adresinin bildirilerek üyelik hesabı açılmaksızın misafir müşteri girişi ile oluşturulduğu ve e-posta ile SMS gönderimi için açık rızanın verildiği,

Üyelik hesabı açmadan oluşturulan siparişlerde kullanıcıların "Kişisel verileriniz, Kişisel Verilerin Korunmasına İlişkin Aydınlatma Metni kapsamında işlenmektedir." bilgisi ile karşılaştığı ve burada aydınlatma yükümlülüğünün yerine getirilmesini sağlayan konularda bilgilendirmelerde bulunulduğu, ilgili kullanıcıların siparişin bir sonraki adımına geçmeyi kabul etmeleri halinde kişisel verilerinin işlendiği,

İlgili kişinin veri sorumlusuna yaptığı başvuruda kendisine reklam içerikli e-posta gönderilmemesi ile ilgili olarak herhangi bir talepte bulunmadığı,

Tüm müşterilere diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkan sağlandığı ve veri sorumlusu tarafından gönderilen tüm ticari elektronik iletilerde bu hususun yer aldığı, ayrıca bu yöndeki şikayetlerin muhatabının da Kurum değil Ticaret Bakanlığının il ve ilçe müdürlükleri olduğu,

Şikayete konu somut olayda, bir başka gönderici tarafından sehven ilgili kişinin e-posta adresinin sisteme girilmesi, ilgili kişiye ait e-posta adresinin ilgili kişiye ait herhangi bir kayıtla eşleşmemesi ve veri sorumlusunun bu olayda kastının bulunmadığı dikkate alındığında Kanun'un 12'nci maddesinin ihlal edildiğinden söz edilemeyeceği,

Diğer yandan üye olmaksızın misafir müşteri girişi ile yapılan alışverişler esnasında alışveriş yapan kişi tarafından kendisine ait e-posta veya telefon numarası girilmek istenirken sehven hatalı olarak girilen başkalarına ait e-posta ve telefon numaralarının e-ticaret sitesi tarafından teyit edilebilmesine yönelik olarak da teknik geliştirme yapılması çalışmalarına başlandığı ve tamamen kontrol dışında gerçekleşen bu durumun önüne geçmek ve hatalı veri girişlerini engellemek amacıyla planlamaların yapıldığı ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/774 sayılı Kararı ile;

6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen

otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

Kanun'un 5'inci maddesinin kişisel verilerin işlenme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı

Buna göre;

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin Kanuna aykırı bir biçimde işlendiğine yönelik iddiası hakkında;

Veri sorumlusunun, müşterilerine üye olma seçeneği sunduğu, bu kapsamda üyelik oluşturan kişilerden manuel girilebilecek şekilde e-posta bilgisini beyan etmelerini istediği, veri sorumlusu tarafından üyeliği olmayan müşterilere de hizmet verildiği, üyelik kaydı bulunmaksızın sipariş oluşturan müşterilerden gerek hizmetin ifası gerekse e-faturanın gönderilmesi gibi amaçlarla e-posta bilgisinin yine manuel olarak girilebilecek şekilde beyan etmelerinin istendiği,

Veri sorumlusu tarafından, ilgili kişinin üyelik bilgilerinde yalnızca "xxx" e-posta adresinin olduğu, ilgili kişi ile aynı isme sahip üçüncü kişinin üyelik oluşturmadan misafir müşteri girişi ile ilgili kişiye ait bir diğer e-posta adresi olan "yyy" adresini sehven girerek sipariş verdiği, "yyy" e-posta adresi için ilgili kişi veya bir başka kişi için üyelik hesabı bulunmadığı, e-postanın ilgili kişiye ait herhangi bir veriyle eşleşmediği veya ilgili kişiye ait kimlik bilgilerinin işlenmediği, misafir müşteri girişi ile yapılan alışverişler esnasında girilen e-posta ve telefon numaralarının teyit edilebilmesine yönelik olarak henüz bir kontrol mekanizmasının bulunmadığının belirtildiği, veri sorumlusunun cevabi yazı eki incelendiğinde de, ilgili kişinin üyelik bilgisinde "xxx" e-posta adresinin olduğu ve sistemlerinde "yyy" e-posta adresinin yer almadığının görüldüğü, diğer yandan ilgili kişinin şikayet ekinde "yyy" e-posta adresine kendisi tarafından oluşturulmayan bir siparişe dair e-ticaret sitesi tarafından bilgilendirme e-postasının gönderildiğine ilişkin ekran görüntülerinin yer aldığı,

İlgili kişiye gönderilen sipariş bilgilendirme e-postasında; söz konusu siparişe dair detayların bulunduğu, hediye olarak gönderilen bu siparişte gönderici adının ve cep telefonu numarasının yer aldığı, bunun yanında alıcı adının, cep telefon numarasının ve adresinin açıkça yer aldığı,

Bireyler tarafından manuel olarak yapılan bilgi girişlerinde yanlış beyanlarda bulunulabilmesinin muhtemel olduğu, veri sorumluları tarafından ise Kanun'un 12'nci maddesinin (1) numaralı fıkrasında tanımlanan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik idari ve teknik tedbirlerin alınması yükümlülüğü kapsamında, bu yanlış bilgi girişleri sebebiyle üçüncü kişilere ait kişisel verilerin hukuka aykırı bir

biçimde işlenmesinin önüne geçilebilmesi adına, kendilerine bildirilen iletişim bilgilerinin doğruluğunu teyit edecek mekanizmaların oluşturulmasına yönelik gerekli idari ve teknik tedbirlerin alınması gerektiği,

Dolayısıyla somut olayda şikayete konu siparişin kendisi tarafından verilmemesine karşın ilgili kişinin kişisel verisi niteliğindeki "yyy" e-posta adresine veri sorumlusu tarafından bilgilendirme e-postası gönderilmek suretiyle kişisel veri işleme faaliyetinde bulunulduğu, bu işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği,

Bu çerçevede söz konusu işlemde bir teyit mekanizmasının bulunmaması nedeniyle e-ticaret sitesine üye olmadan misafir girişi ile yapılan tüm alışveriş işlemlerinin veri ihlal riski taşıdığı,

Bilgilendirme e-postalarının, gönderici ve alıcılara ait ad, soyad, T.C. kimlik numarası, adres, telefon, e-posta, sipariş bilgileri gibi bilgileri ihtiva edebileceği, bilgilendirme e-postasının konu ile ilgisiz üçüncü bir kişiye gönderilmesinin, konu ile ilgisiz üçüncü kişinin kişisel verisinin hukuka aykırı bir biçimde işlenmesi sonucunu doğurduğu gibi içerikte yer alan kişisel verilerin olduğu gibi üçüncü bir kişiye açıklanarak bu verilerin başkaları tarafından kötü niyetli olarak kullanılmasına da zemin hazırlayabileceği,

İlgili kişinin Kanun kapsamında yaptığı başvuruya veri sorumlusu tarafından cevap verilmediğine yönelik iddiası hakkında:

İlgili kişinin Kanun kapsamında başvuru yapmak maksadıyla doldurduğu başvuru formu ile veri sorumlusunun cevabi yazı ve ekinde yer alan bahse konu belgeler incelendiğinde ve gönderi takip formunda yer alan gönderi barkod numarası sorgulandığında; başvuruya verilecek yanıtın tarafına bildirilme yöntemi olarak yalnızca "Adresime gönderilmesini istiyorum" kutucuğunu işaretlediği, veri sorumlusu tarafından ilgili kişiye cevap verildiği, bu cevabın ilgili kişinin belirttiği şekilde adresine teslim edildiğinin görüldüğü, bu sebeple veri sorumlusu tarafından ilgili kişinin yaptığı başvuruya cevap verildiğinin anlaşıldığı,

İlgili kişinin e-posta adresine veri sorumlusu tarafından kendisine ait e-posta adresinin silindiğinin ve artık kendisine bildirim iletilmeyeceğinin ifade edilmesine rağmen halen reklam içerikli e-postaların iletildiğine yönelik iddiası hakkında:

İlgili kişinin şikayet dilekçesi ve ekinde; söz konusu siparişe dair gönderilen bilgilendirme e-postalarının, bunun üzerine e-ticaret sitesi asistanı üzerinden gerçekleştirmiş olduğu görüşme trafiğinin ekran görüntüsünün ve Kanun kapsamında yapmış olduğu başvurusunun yer aldığının görüldüğü, veri sorumlusunun cevabi yazı ekinde, bu belgelerin yanı sıra ilgili kişiye verilen yanıtın yer aldığı dokümanlar incelendiğinde; bahse konu siparişten ilgili kişinin kişisel verisi niteliğindeki e-posta adresinin silindiğinin ve kendisine bildirim iletilmeyeceğinin müşteri hizmetleri ile yapılan görüşmede ifade edildiği, bununla birlikte ilgili kişinin veri sorumlusuna başvurusunda halen kendisine reklam içerikli e-postanın iletilmeye devam edildiğine dair bir ifadesine rastlanılmadığı ve ilgili kişinin Kuruma ilettiği şikayetinde reklam içerikli e-posta iletilmeye devam edildiği iddiasına yönelik tevsik edici herhangi bir bilgi ve belgeye yer verilmediği,

Veri sorumlusunun tüm müşterilere diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkan sağlandığına, e-ticaret sitesi tarafından gönderilen tüm ticari elektronik iletilerde sunulan bu imkanın belirtildiğine, bu yöndeki şikayetlerin muhatabının Kurumun değil Ticaret Bakanlığının il ve ilçe müdürlüklerinin olduğuna yönelik açıklamaları hakkında:

Telefon ve e-posta bilgisinin bir iletişim bilgisi olduğu, bu iletişim bilgilerinin kişisel veri olduğu, kişisel veriler üzerinde Kanun'da belirtilen yollarla gerçekleştirilen her türlü işlemin bir işleme faaliyeti olduğu, bu bilgilerin kişiyi belirlenebilir kılmak maksatlı işlendiği, dolayısıyla SMS ya da e-posta yoluyla ticari elektronik ileti gönderilmesi suretiyle bir kişinin e-posta ya da cep telefonu bilgisinin kullanılmasının bir kişisel veri işleme faaliyeti olduğu ve kişisel verilerin hangi işleme şartlarına dayalı olarak işlenmesi gerektiğini düzenleyen Kanun kapsamında değerlendirileceği değerlendirmelerinden hareketle;

Veri sorumlusu tarafından taraflara yönelik bir teyit mekanizması kurulmadan satış sözleşmesi ile ilgisiz üçüncü kişi konumundaki ilgili kişiye sipariş bilgilendirmesine dair e-posta gönderilmesi suretiyle kişisel verisinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi birine dayanılmaksızın işlendiği, bu bakımdan Kanun'un 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmediği kanaatine

varıldığından, veri sorumlusunun 550+ çalışan ve 40.000+ tedarikçi ağından oluşan bir ekiple süreçlerini yürütmekte olduğu, şikayete konu olayda veri sorumlusunun Kanun'un 12'nci maddesindeki yükümlülüklerini yerine getirmeyerek ihmali davranışla e-postanın gönderileceği alıcı gruplarına yönelik bir teyit mekanizması kurmadan uzaktan satış sözleşmesinin tarafı olmayan ilgili kişinin e-posta adresinin işlenmesine, dolaylı olarak e-postada yer alan gönderici ve alıcıya ait bilgilerinin ise ilgili kişiye açıklanmasına sebebiyet verildiği, bu e-postanın yanlış muhataba gönderilmesi halinde hak kaybına yol açabileceği hususları da dikkate alınarak, veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 120.000 TL idari para cezası uygulanmasına,

İlgili kişinin Kanun kapsamında yapmış olduğu başvuruya veri sorumlusu tarafından yasal süreler içinde cevap verildiğinin görülmüş olması sebebiyle ilgili kişinin veri sorumlusu tarafından başvuruya cevap verilmediği iddiasına yönelik olarak veri sorumlusu hakkında Kanun kapsamında yapılacak herhangi bir işlem olmadığına karar verilmiştir.

KARAR 3:

KIŞISEL VERILERI KORUMA KURUMU

Tüketici finansman kredisiyle alışveriş imkanı sunan şirket tarafından ilgili kişilerden E-Devlet şifrelerinin talep edilmesi

(6698 S. K. m. 3, 5, 7, 12, 18) (Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik m. 5, 6)

Karar Tarihi: 22/03/2023

Karar No: 2023/426

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Kuruma intikal ettirilen bir ihbar dilekçesinde özetle;

Tüketici finansman kredisiyle alışveriş imkânı sunan Şirketten senetle televizyon alındığı sırada kendisinden e-Devlet şifresinin talep edildiği,

Kuruma intikal ettirilen bir diğer ihbar dilekçesinde ise özetle;

Şirketin ihbar edenden e-Devlet şifresini istediği, ihbar edenin ısrarlar sonucunda şifre almadığını söyleyerek talebi reddettiği,

İhbar edenin kendisi dışında birçok vatandaştan da e-Devlet şifrelerinin alındığının bilindiği hususları belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan resen inceleme çerçevesinde ihbar edilen veri sorumlusu Şirketin savunması talep edilmiş olup veri sorumlusunun ilk ihbar dilekçesine ilişkin cevabî yazısında özetle;

İhbar edenin veri sorumlusu ile tüketici finansman sözleşmesi akdetmiş olduğu, kredi puanı yetersiz görüldüğünden ve işyerinde sigorta girişinin yeni yapıldığını belirtmesi üzerine son altı aylık güncel sigorta hizmet dökümü belgesi ile şubeye müracaat edilmesinin istendiği ve fakat ihbar eden kişi tarafından sözleşmenin iptal edildiği,

İhbar edenin ürün satın almak için başvuruda bulunduğu, işlem yapmak amacıyla açık rızası ile irtibat numarasını bildirmiş olduğu, Şirketin Tüketici Finansman Kredisi kullanılmasına ilişkin ihbar edenin yeni işe başladığını beyan etmesi üzerine işe başlama kaydının sigorta hizmet dökümü üzerinden teyit edilmesi amacıyla müşterinin en yakın şubeye davet edildiği ve sigorta kayıtlarının beyan edilmesinin talep edildiği, bu bilgilerin e-Devlet sistemi üzerinden temin edileceğinin sabit olduğu, şirketin ihbar edenin e-Devlet şifresini talep etmediği, ilgili kişinin e-Devlet şifresinin bilinmediği, müracaat anında müşterinin sigorta hizmet dökümünü görüntülemek, işe başladığını teyit etmek ve öğrenebilmek adına kendi rızası olduğu takdirde ve kendi cep telefonundan kendisinin görebileceği şekilde e-Devlet üzerinden talep edilen kayıtların gösterilmesinin talep edildiği, müşteri/ihbar edenin ilgili kayıtları paylaşmadığı ve sözleşmenin iptalini talep ettiği,

İhbar edenin kişisel verilerinin işlenmesinin gerekçelerinin ise; şirketin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, tüketici sözleşmesinin kullanımı açısından sigorta hizmet dökümü bilgisinin talep edilmesinin zorunluluğu, bir hakkın tesisi, kullanılması veya korunması için bilgi talebi olması, şirketin meşru menfaatleri için bilgi talebinin gerekli olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait bilgi talebinin gerekli olması olduğu belirtilmiştir.

Aynı konuya ilişkin veri sorumlusu Şirketin ikinci ihbar dilekçesine ilişkin cevabî yazısında ise özetle;

Somut olayda ihbar edenin veri sorumlusu ile taksitli satış sözleşmesi akdettiği, sonrasında bozuk olan ürün yerine yeni ürünün ilgili kişiye teslim edildiği, ardından bu üründe de arıza olunca ürün satış işleminin iptal olduğu ve ücret ödemesinin ihbar edene iade edildiği,

Veri sorumlusunun, ilgili mevzuat çerçevesinde yükümlülüklerini yerine getirmek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almış olduğu,

Müşterilerden/ilgili kişilerden e-Devlet şifresi talep edildiği yönündeki iddiaların gerçek dışı olduğu, veri sorumlusunun Kanun gereğince, tüketici işlemleri sırasında herhangi bir veri tutmadığı; kimlik aslının ve iletişim bilgilerinin ilgili kişilerden kontrol amacıyla alındığı ve yapılan kontrollerin ardından kimlik aslının geri verilip suretinin dahi sistemlerde kayıt altına alınmadığı,

İddia edildiği gibi e-Devlet şifresi ile taksitli satış sözleşmesi arasında bir illiyet bağının olmadığı, e-Devlet şifresi ile satış sözleşmesi arasında birbiri ile ilişkili bir işlemin söz konusu olmadığı, e-Devlet şifresi ile yapılacak bir işlemin de bulunmadığı,

Kişisel verilerin korunması ve işlenmesi konusunda azami düzeyde teknik ve idari tedbirleri alan veri sorumlusunun, e-Devlet gibi kişiye ait özel bir alanı kullandığı iddiasının Şirket politikası ve uygulamaları ile ters düşeceği, bu açıdan hiçbir müşteriden herhangi bir şifre talep etme durumunun söz konusu olmadığı, somut durumlar karşısında Şirket açısından herhangi bir cezai yaptırım oluşturabilecek bir durumun söz konusu olmadığı belirtilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 22/03/2023 tarihli ve 2023/426 sayılı Kararı ile;

Kişilerin kendilerine ait ad-soyadı, iletişim numarası gibi tüketici işlemlerinde kullanılan bilgilerin veri sorumlusunun veri kayıt sisteminde işlenmesinden ötürü, Kanunun 2'nci maddesinde yer alan hüküm dikkate alındığında Kuruma yapılan ihbarların Kanun kapsamında olduğu,

Kanunun 3'üncü maddesinin birinci fıkrasının (ç) bendi gereği Şirket'in veri kayıt sisteminde kişisel verileri tutulan ihbarda bulunanların ilgili kişi, (ı) maddesi gereği ilgili kişilerin kişisel verilerinin işlenme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin tutulmasından ve yönetilmesinden sorumlu tüzel kişi olan Şirket'in ise veri sorumlusu olduğu,

Kişisel verilerin işlenme şartlarının Kanun'un 5'inci maddesinde düzenlendiği; buna göre maddenin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında -Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinden birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun düzenlendiği,

İlgili kişinin Kuruma sunduğu ihbar dilekçesinde Şirketten senetle televizyon alındığı ve kendisinden e-Devlet şifresinin talep edildiğinin ifade edildiği, başvuru ekinde yer alan ve Şirket tarafından ilgili kişinin cep telefonu numarasına gönderildiği anlaşılan kısa mesajda "E-Devlet şifreniz ile beraber en yakın şubemize gelmenizi rica ederiz. (Sipariş no, kayıt tarihi:16.01.2022, ürünler başlıkları ile)" ifadelerinin yer aldığının görüldüğü,

Veri sorumlusunun savunmasında; ihbar edenin Şirket ile tüketici finansmanı sözleşmesi akdetmiş olduğu, kredi puanı yetersiz görüldüğünden ve işyerinde sigorta girişinin yeni yapıldığını belirtmesi üzerine son altı aylık güncel sigorta hizmet dökümü belgesi ile şubeye müracaat etmesinin istendiği ve ilgili kişi tarafından sözleşmenin iptal edildiği, tüketici sözleşmesinin kullanımı açısından sigorta hizmet dökümü bilgisinin talep edilmesinin zorunlu olduğu, bu bilgilerin e-Devlet sistemi üzerinden temin edileceği, e-Devlet şifresinin talep edilmediği, müracaat anında müşterinin sigorta hizmet dökümünü

görüntülemek, işe başladığını teyit etmek ve öğrenebilmek adına şifreyi kendi rızası olduğu takdirde ve kendi cep telefonundan kendisinin görebileceği şekilde e-Devlet üzerinden girmek suretiyle talep edilen kayıtların gösterilmesinin istendiği, ilgili kişinin kayıtları paylaşmadığı ve sözleşmenin iptalini talep ettiği hususlarını belirtmiş olduğu,

İlgili kişi ve veri sorumlusunun beyanları ile Kuruma sunulan belgelerden; ilgili kişinin veri sorumlusu ile tüketici finansmanı (kredisi) sözleşmesi yaptığı, ilgili kişiye iletilen kısa mesajda ilgili kişinin e-Devlet şifresi ile beraber şubeye çağırıldığı, ilgili kişinin ise e-Devlet şifresinin kullanılmasına yönelik rızası olmadığından sözleşmeyi iptal etmek istediğinin anlaşılmakta olduğu,

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerektiği, bu riskler belirlenirken kişisel verilerin özel nitelikli kişisel veri olup olmadığı, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliğinin dikkate alınması gerektiği, bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatiflerinin maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmesi ve gerekli teknik ve idari tedbirlerin planlanarak uygulamaya konulması gerektiği,

Bununla birlikte Kişisel Veri Güvenliği Rehberi'nde veri sorumlularınca alınabilecek idari tedbirlerin; "kişisel veri işleme envanteri hazırlanması, kurumsal politikalar (erişim, bilgi güvenliği, kullanım, saklama ve imha vb.), sözleşmeler (veri sorumlusu-veri sorumlusu, veri sorumlusu-veri işleyen arasında), gizlilik taahhütnameleri, kurum içi periyodik ve/veya rastgele denetimler, risk analizleri, iş sözleşmesi, disiplin yönetmeliği (kanuna uygun hükümler ilave edilmesi), kurumsal iletişim (kriz yönetimi, kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.), eğitim ve farkındalık faaliyetleri (bilgi güvenliği ve kanun), veri sorumluları sicil bilgi sistemine (VERBİS) bildirim" şeklinde örnek teşkil etmesi amacıyla ifade edildiği,

Bu kapsamda, ihbara konu edilen e-Devlet şifresi istenmesi beyanına ilişkin gerek resen inceleme kapsamındaki ihbarlar gerekse veri sorumlusuna ilişkin kamuya açık kaynaklarda yer alan şikayetler ele alındığında veri sorumlusunun kişisel veri işleme faaliyetlerinin kontrolünü sağlayamadığına, dolayısıyla gerekli teknik ve idari tedbirleri almadığına ilişkin güçlü bir kanaat oluştuğu, bilhassa senetli alışverişlerde müşterilerin e-Devlet şifrelerinin temin edilmesi suretiyle ilgili kişilerin e-Devlet kapısında yer alan kendileriyle ilgili her türlü bilgiye veri sorumlusunca erişilebilme tehlikesi ile karşı karşıya kalacakları; ayrıca veri sorumlusunun ihbara konu olayda veri güvenliğinin sağlandığına yönelik yeterli bilgi ve belgeyi de sunamadığı,

Öte yandan veri sorumlusunun e-Devlet şifrelerinin talep edilmesine ilişkin savunmasında, bir taraftan ilgili kişiler ile akdettiği tüketici kredisi sözleşmesi sebebiyle işe başlama kaydının sigorta hizmet dökümü üzerinden teyit edilmesi amacıyla müşteriyi en yakın şubeye davet ettiğini belirtirken diğer taraftan e-Devlet şifresi ile taksitli satış sözleşmesi arasında bir illiyet bağının olmadığını, e-Devlet şifresi ile satış sözleşmesi arasında birbiri ile ilişkili bir işlemin söz konusu olmadığını, e-Devlet şifresi ile yapılacak bir işlemin de bulunmadığını ifade etmiş olduğu,

Resen inceleme kapsamındaki iki dosyaya ilişkin veri sorumlusunca -aynı konu kapsamında- Kuruma sunulan bilgi ve belgelerin bütünlük ve tutarlılık içinde olmadığı, kişisel verilerin işlenmesi suretiyle kurulan sözleşmelere ilişkin hususların Kanun kapsamında ifade edilemediği,

Veri sorumlusu tarafından yürütülen veri işleme faaliyetlerinde ilgili kişilerden e-Devlet şifresi talep edilmesine ilişkin kamuoyuna yansıyan çok sayıda şikayet olduğu, resen inceleme dosyalarında veri sorumlusu tarafından e-Devlet şifresi hakkında sunulan beyanların da birbiri ile tutarlı bir çerçevede olmadığı, veri sorumlusunun ülkemizde çok sayıda mağazası olan - tüketici finansman kredisiyle alışveriş imkânı sunan/taksitle satış yapan- bir şirket olduğu, Kuruma sunulan ihbarlar dışında taksitli satışlarda ilgili kişilerden e-Devlet şifresi istendiğine ilişkin şifahi bilgiler de edinildiği, e-Devlet şifresinin ele geçirilmesi durumunun veri güvenliğine yönelik ciddi riskler ortaya çıkarabileceği hususlarının tümünün idari teknik tedbirleri alma noktasında eksikliği olduğu kanaatine

varılan veri sorumlusu hakkında uygulanacak idari yaptırımda artırım sebepleri olarak ele alınabileceği,

İnternette yer alan açık kaynaklarda, veri sorumlusundan yapılan taksitli alışverişlerde ilgili kişilerin e-Devlet şifrelerinin alındığına dair pek çok şikayet olduğunun görülmesi, konuya ilişkin Kuruma da intikal eden farklı şikayetler olması, e-Devlet şifrelerinin talep edildiği her olayda tüm müşterilerin e-Devlet şifrelerini kendi telefonlarından açıp göstermesinin söz konusu olmayabileceği dikkate alındığında Şirket bilgisayarları aracılığıyla görüntüleme yapılmış olmasının mümkün olduğu değerlendirmelerinden hareketle;

İlgili kişilerin e-Devlet şifrelerine erişim sağlandığı yönünde güçlü bir kanaat oluştuğu, ilgili kişilerin e-Devlet şifreleri talep edilerek hassas nitelikli olanlar da dahil pek çok kişisel veriye erişim sağlanabileceği sonucuna varıldığından veri sorumlusundan yapılan taksitli alışverişlerde e-Devlet şifrelerinin talep edilmesinin Kanun'un 5'inci maddesinde yer alan herhangi bir veri işleme şartına dayanmaması nedeniyle Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmediği değerlendirilen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL idari para cezası uygulanmasına,

Hukuka aykırı işlendiği değerlendirilen kişisel verilerin Kanun'un 7'nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca imha edilerek sonucundan Kurula bilgi verilmesine karar verilmiştir.

KARAR 4:

KIŞISEL VERILERI KORUMA KURUMU
Kişinin E-posta adresine başka abonelere ait E-faturaların gönderilmesi
(6698 S. K. m. 4, 12, 18)
Karar Tarihi: 08/09/2022
Karar No: 2022/925

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; ilgili kişinin daha önce veri sorumlusu telekomünikasyon şirketi hakkında kendisine ait e-posta adresine başka bir aboneye ait e-faturaların gönderilmesi nedeniyle şikâyette bulunduğu, bu kapsamda veri sorumlusu telekomünikasyon şirketi hakkında Kişisel Verileri Koruma Kurulu (Kurul) tarafından idari para cezası uygulanmasına ve kişisel verilerin güvenliğine ilişkin gerekli tüm idari ve teknik tedbirlerin alınması hususunda veri sorumlusunun talimatlandırılmasına karar verildiği ancak 2018 yılından beri 053.….4 numaralı hattın sahibinin e-faturalarının veri sorumlusu tarafından ilgili kişiye iletildiği bununla birlikte 054…...9 numaralı hattın sahibinin e-faturalarının da kendisine iletilmeye başlandığı ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

Öncelikle ilgili kişiye ait verilerin düzeltilmesini isteme hakkının yerine getirilmediği iddiasının gerçeği yansıtmadığı, ilgili kişinin şirkete yaptığı başvuru sonrasında 054……9 numaralı hattın faturalama bilgilendirme tercihinin Mayıs 2020 dönemi ve sonrası için e-faturadan SMS'e çevrildiği; bu çerçevede, şirket sistemlerinde yapılan sorgulamada 054……9 numaralı telefon numarasına ilişkin hazırlanan e-faturanın ilgili kişinin beyan ettiği e-posta adresine en son 30 Nisan 2020 tarihinde iletildiğinin tespit edildiği,

Aynı e-mail adresini beyan eden 053……4 numaralı hat sahibine ise konuya ilişkin olarak ulaşılmaya çalışılmasına rağmen borcundan dolayı hattının erişime kısıtlı olması nedeniyle ulaşılamadığı, abonelik sözleşmesi kapsamında aynı e-posta adresini beyan eden hat sahibinin değişikliğe ilişkin rızası alınamadığı için herhangi bir işlem yapılamadığı, hat sahibinin abonelik sözleşmesinde beyan ettiği bilgilerin hat sahibinin iradesi dışında değiştirilmesinin Kanun kapsamındaki haklarının ihlaline ve Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) ilgili yönetmeliklerine aykırı hareket edilmesine sebep olacağı, zira kişisel verilerinin düzeltilmesinin kullanılması hakkının hat sahibine ait olduğu,

İlgili kişinin ilk şikâyetini 11.01.2019 tarihinde Kuruma iletti̇ği, ilk başvurusunda, yalnızca 053……7 numaralı hattın faturalarının kendisine gönderilmesi ve bu suretle e-posta adresinin hukuka aykırı işlendiğine ilişkin rahatsızlığını beyan ettiği ancak 053……4 numaralı hatta ait faturaların da 2018 yılında aynı e-posta adresine iletilmekte olduğu görülmesine rağmen ilgili kişinin yaptığı 11.01.2019 tarihli ilk başvuruda 053…..4 numaralı hattın faturasına ilişkin rahatsızlık duyduğunu beyan etmediği, ilk başvurusunda yer vermediği bu numaraya yönelik rahatsızlığını yaklaşık 18 ay sonra iletme gereği duymasının diğer şikâyetlerinde kullanmak üzere numarayı elinde tutmayı tercih etmesi anlamına geldiği, gereksiz iş yükü getiren ve etik olmayan bu tercihin dürüstlük ilkesiyle bağdaşmadığı ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kurulun 08/09/2022 tarih ve 2022/925 sayılı Kararı ile;

Kanun'un "Genel İlkeler" başlıklı 4' üncü maddesinde "(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." hükmünün yer aldığı

Kanun'un "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinde; "(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne yer verildiği,

Somut olayda ilgili kişinin ilk başvurusuna istinaden verilen Kurul Kararı kapsamında veri sorumlusunun kişisel verilerin güvenliğine ilişkin gerekli tüm idari ve teknik tedbirlerin alınması hususunda talimatlandırılmasına rağmen, üçüncü kişilere ilişkin faturanın ilgili kişinin e-posta adresine iletilmeye devam edilmesinin ve yine üçüncü bir kişiye ait abonelik sözleşmesinde ilgili kişinin e-posta adresinin bildirilmiş olmasının, mevcut ve yeni üyelerin e-posta adresi gibi iletişim kanallarının doğrulanmasına yönelik bir mekanizmanın bulunmadığını gösterdiği,

Veri sorumlusunun söz konusu kişisel verilerin doğruluğunu sağlamak amacıyla proaktif bir yaklaşımla gerekli tedbirleri almamasının Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil ettiği, dolayısıyla veri sorumlusu tarafından kişisel verilerin işlenmesinde Kanun'un 12'nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirlerin alınmadığı kanaatine varıldığı değerlendirmelerinden hareketle;

İlgili kişinin e-posta adresinin üçüncü kişilere ait faturanın iletilmesi suretiyle işlenmesi ve bu durumun Kanun'un 4 üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil etmesi sebebiyle Kanun'un 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülükleri yerine getirmediği kanaatine varılan veri sorumlusu hakkında, daha önce verilen Kurul Kararında abonelerin kişisel verilerinin güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınması hususunda talimatlandırıldığı da dikkate alınarak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,

İlgili kişinin e-posta adresine üçüncü kişilere ait kişisel verilerin iletilmemesi amacıyla gerekli tedbirlerin alınması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

KARAR 5:

KIŞISEL VERILERI KORUMA KURUMU

İlgili kişinin kredi notunun banka tarafından düzeltilmemesi ve kişisel verilerinin üçüncü kişilerle paylaşılması

(6698 S. K. m. 3, 4, 5, 6, 8, 11, 12, 18) (5411 S. K. Ek m. 1, Geç. m. 28) (Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği m. 9, 10, 17)

KVKK KURUL KARAR ÖZETLERİ

Karar Tarihi: 02/11/2021

Karar No: 2021/1107

Konu Özeti: İlgili kişinin kredi notunun Banka tarafından düzeltilmemesi ve kişisel verilerinin üçüncü kişilerle paylaşılması

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Kuruma intikal eden şikâyette özetle; ilgili kişi tarafından bireysel kredi kartı ödemesi geciktirilmediği hâlde veri sorumlusu Banka tarafından kanuni takip başlatıldığı ve defalarca ilgili kişinin kredi notunu etkileyen hukuksuz işlemler yapıldığı, ilgili kişinin kredi notunun düşürüldüğü, yapılan itiraz üzerine Banka tarafından bu işlemin düzeltildiği ve kredi notunun yüksek düzeye yeniden çekildiği fakat bu işlemin takip eden aylarda Banka tarafından birkaç kez daha tekrarlandığı ve her seferinde ilgili kişinin ısrarlı tepkileri sonucunda düzeltildiği, finans bilgilerinin gerçeğe aykırı olarak hukuksuz bir biçimde paylaşıldığı, ilgili kişi ile hiçbir finans kurumu arasında kredi, bireysel kart vb. gibi işlemlerin yapılamadığı, ilgili kişinin itibarının zedelendiği ve Bankaya yapılan başvurulara yanıt verilmediği belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun Kuruma intikal eden cevabi yazısında özetle;

İlgili kişinin bahsettiği tarihte başvurusunun bulunmadığı fakat başka bir tarihte kendilerine e-posta üzerinden bir şikâyet ilettiği ve aynı tarihte kendisi ile telefonla irtibata geçildiği fakat ilgili kişinin aramaları yanıtlamaması nedeniyle kendisine e-posta ile bilgi verilerek görüşme talebinde bulunulduğu ancak Banka tarafından iletilen e-postaya ilgili kişiden herhangi bir yanıt alınamadığı ancak aynı konulu başka tarihteki şikâyetlerinin Banka Genel Müdürlüğüne iletilerek başka bir tarihte yanıtlandığı,

Banka ile kurumlar arasında imzalanan protokoller kapsamında kurumların fatura tahsilatlarına aracılık hizmetinin verildiği ve bu kapsamda ilgili kişinin imzalamış olduğu Bankacılık Hizmetleri Sözleşmesi çerçevesinde verdiği fatura ödeme talimatlarının yerine getirilebilmesi amacıyla fatura ödeme talimatı verilen kurumlarla müşteri işlem; Banka nezdinde kredi ürünlerine ilişkin olarak bankacılık sektörüne yönelik yasal düzenlemelere uyumun sağlanması, Bankanın risk izleme ve bilgilendirme yükümlülüklerinin yerine getirilmesi amacıyla Türkiye Bankalar Birliği Risk Merkezine kimlik, iletişim, müşteri işlem; Banka'nın acentesi olduğu …Sigorta A.Ş. nezdindeki sigorta poliçelerinin prim ödemeleri ile ilgili olarak söz konusu Şirkete müşteri işlem; ilgili kişinin yasal takipte izlenen kredilerinden kaynaklanan Bankanın alacaklarının tahsili amacıyla anlaşmalı hukuk bürosuna kimlik, iletişim, müşteri işlem, hukuki işlem bilgilerine ilişkin olarak her bir konu özelinde, ilgili amacın gerçekleştirilmesiyle kısıtlı olacak şekilde veri aktarımının gerçekleştirildiği,

İlgili kişinin yurt dışına aktarılan kişisel verisinin bulunmadığı,

19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu'nun Geçici 28'inci maddesinde Türkiye Cumhuriyet Merkez Bankası nezdinde izlenen risk verilerinin 5411 sayılı Kanun'a göre kurulmuş olan Risk Merkezine aktarılmasının düzenlendiği, aynı Kanun'un Ek 1'inci maddesinde ise; "Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur." düzenlemesinin yer aldığı, anılan hükümler ve Türkiye Bankalar Birliği tarafından yayımlanan Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği ile üye bankaların Risk Merkezine bilgi paylaşımının kapsamı, biçimi ve içeriği ile tarafların yükümlülüklerinin düzenlendiği,

İlgili kişinin talebi üzerine yapılan incelemede gerçek kişi tacir ilgili kişinin bireysel kredi kartı geri ödemelerinde gecikme olmamasına karşın ticari nitelikli kredi kartından kaynaklanan gecikme nedeniyle gecikme bildiriminin yapıldığının anlaşıldığı,

Bu durumun giderilmesine yönelik olarak gerekli sistem geliştirmesinin planlandığı ve 2020 yılı Mayıs ayı içerisinde gerçekleşecek sistem güncellemesi sonrasında aktif hale geleceği ve konu hakkında Kuruma ayrıca bilgi verileceği, çalışmalar tamamlanıncaya kadar ilgili kişiye ilişkin kayıtların manuel olarak kontrol edilmeye ve gerekirse düzeltilmeye devam edileceği,

Güncelleme işlemlerinin Türkiye Bankalar Birliği Risk Merkezine ait portal üzerinden, kullanıcı ve onaylayıcı olarak yetkilendirilmiş Banka çalışanlarının Bankanın sistemindeki güvenlik kontrollerine uygun şekilde giriş yapması sonrasında gerçekleştirilebildiği, Portaldaki "Acil Güncelleme Sistemi"ne müşteri T.C. kimlik numarası bilgisinin girilerek gerekli düzeltmenin yapıldığı ve yetkilendirilmiş kullanıcının onayıyla sürecin tamamlandığı ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1107 sayılı Kararı ile;

Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

şeklinde sayıldığı,

Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

Kanun'un "Kişisel verilerin aktarılması" başlıklı 8'inci maddesinde; kişisel verilerin ilgili kişilerin açık rızası olmaksızın aktarılamayacağının, özel nitelikli olmayan kişisel verilerin ancak Kanun'un 5'inci maddesinin (2) numaralı fıkrasında belirtilen şartlardan birinin varlığı halinde, özel nitelikli kişisel verilerin ise yeterli önlemler alınmak kaydıyla 6'ncı maddesinin (3) numaralı fıkrasında belirtilen şartlardan birinin bulunması halinde ilgili kişinin açık rızası aranmaksızın aktarılabileceğinin düzenlendiği,

Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

5411 sayılı Kanun'un Geçici 28'inci maddesinin üçüncü fıkrasında; "Merkez Bankası nezdindeki Risk Merkezi bilgileri, bu Kanuna göre kurulan Risk Merkezine aktarılır." hükmü ile aynı Kanun'un Ek 1'inci maddesinde; Risk Merkezine ilişkin ayrıntılı düzenlemelere yer verildiği, ilgili hükmün birinci fıkrası uyarınca Risk Merkezinin; Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Bankacılık Düzenleme ve Denetleme Kurulu tarafından uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay

vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere kurulmuş olduğu, bu maddenin ikinci fıkrası gereğince; kredi kuruluşları ile Bankacılık Düzenleme ve Denetleme Kurulu tarafından uygun görülecek finansal kuruluşların, Risk Merkezine üye olmak zorunda olduğu ve üye kuruluşların, Risk Merkezince istenilen, müşterileri ile ilgili her türlü bilgiyi vermekle yükümlü olduğunun düzenlendiği, bu açıklamalarda bahsi geçen kredi kuruluşlarının; 5411 sayılı Kanun'un 3'üncü maddesinde, mevduat bankaları ve katılım bankaları olarak açıklandığı,

10/04/2012 tarihli ve 28260 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Türkiye Bankalar Birliği Risk Merkezi Yönetmeliğinin (Risk Merkezi Yönetmeliği) 9'uncu maddesi gereğince; Risk Merkezine üye olanlar tarafından Risk Merkezine müşteri ve/veya hesap bazında değişiklikler göstermekle birlikte, kredi limiti, kredi riski, donuk alacak niteliğindeki kredi ve diğer alacaklar, çekler ve çek hesabı sahibinin bilgileri vb. ile Risk Merkezi Yönetimi tarafından Risk Merkezinin kuruluş amaçları doğrultusunda belirlenen diğer bilgilerin bildirildiği,

Risk Merkezi Yönetmeliğinin 10'uncu maddesinin birinci fıkrası uyarınca ise; kredi limiti ve kredi riski bilgilerinin müşteri bazında birleştirilerek bu müşteriler hakkında bildirimde bulunan üyelere bildirim dönemi itibariyle topluca bildirildiği, yine aynı Yönetmeliğin 17'nci maddesinin birinci fıkrasının (a) bendinde; Risk Merkezine üye olanların, Risk Merkezi tarafından bu Yönetmelik kapsamında talep edilen her türlü bilgi ve belgeyi zamanında, tam ve gerçeğe uygun olarak vermekle sorumlu olduklarının düzenlendiği,

Somut olayda veri sorumlusunun, banka niteliğini haiz olmakla birlikte 5411 sayılı Kanun'un Ek 1'inci maddesi uyarınca Risk Merkezine üye olma zorunluluğunun bulunduğu ve gerek 5411 sayılı Kanun gerekse Risk Merkezi Yönetmeliği gereğince; Risk Merkezine müşterilerine ait kredi bilgisi, kredi riski vb. bilgileri bildirmesi gerektiği, bu kapsamda ilgili kişiye ait finans verilerinin veri sorumlusu tarafından Risk Merkezine bildirilmesinin Kanun'un 8'inci maddesi anlamında aktarım anlamına gelmekte olduğu ve söz konusu aktarım faaliyetinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından birine dayanması gerektiği,

Bu çerçevede, 5411 sayılı Kanun ile Risk Merkezi Yönetmeliği hükümleri kapsamında veri sorumlusunun söz konusu kişisel veri aktarım faaliyetini gerçekleştirmesi gerektiği, dolayısıyla veri sorumlusunun ilgili kişinin finans verilerini Risk Merkezine bildirmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan; "Kanunlarda açıkça öngörülmesi" ile (ç) bendinde yer alan "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartları kapsamında olduğu,

Kanun'un "Genel ilkeler" başlıklı 4'üncü maddesi uyarınca, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; "a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." şeklinde sayılan ilkelere uyulmasının zorunlu olduğu, anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanun'un 4'üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu,

Bu ilkelerden "Doğru ve gerektiğinde güncel olma" ilkesinin, Kanun'un 11 inci maddesinde düzenleme altına alınan ve ilgili kişinin haklarından biri olan kişisel verilerin düzeltilmesini talep etme hakkı ile doğrudan ilgili olduğu, kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında aktif özen yükümlülüğünün; veri sorumlusu eğer bu verilere dayalı olarak ilgili kişiyle alakalı bir sonuç ortaya koyuyor ise geçerli olduğu (örneğin kredi verme işlemleri),

Somut olay bakımından, kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması bakımından, veri sorumlusu Banka'nın aktif özen yükümlülüğü altında olduğu, zira, kredi verme, kredi kartı kullanımı, hesap özeti çıkarılması gibi işlemler bakımından banka hesap bilgilerinin güncelliğinin önem arz ettiği,

Söz konusu verilerin yalnızca veri sorumlusu bünyesinde tutulmadığı ve pek çok kredi ve finans kuruluşunun erişebildiği Risk Merkezine de aktarıldığı, bununla birlikte, veri sorumlusu Banka'nın, Risk Merkezi Yönetmeliğinin 17'nci maddesinin birinci fıkrasının (a)

bendi gereğince de; Risk Merkezi tarafından bu Yönetmelik kapsamında talep edilen her türlü bilgi ve belgeyi zamanında, tam ve gerçeğe uygun olarak verme sorumluluğu bulunduğu,

Öte yandan, Kanun'un "İlgili kişinin hakları" başlıklı 11'inci maddesi uyarınca; herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, Kanun'un 7 nci maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, 11 inci maddenin birinci fıkrasının (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduğu ve bu kapsamda ilgili kişilerin, kişisel verilerinin eksik veya yanlış işlenmesi halinde, bunların düzeltilmesini talep etme hakkının bulunduğu,

Somut olay bakımından, Kuruma intikal eden belgeler incelendiğinde, veri sorumlusu Banka tarafından ilgili kişiye cevap verildiği ancak konuyu aydınlatacak ve ilgili kişinin şikâyetini çözümleyecek derecede yeterli bir cevap verilmediği,

Zira ilgili kişinin farklı zamanlarda veri sorumlusu ile e-posta yoluyla iletişime geçerek Risk Merkezine yanlış aktarılan finans verilerinin düzeltilmesini tekraren talep ettiğinin görüldüğü,

İlgili kişi tarafından veri sorumlusuna iletilen, sair tarihlerdeki e-postaların tamamının aynı konuya ilişkin olduğu, veri sorumlusu tarafından bu durumun giderilmesine yönelik olarak gerekli sistem geliştirmesinin planlandığı ve 2020 yılı Mayıs ayı içerisinde gerçekleşecek sistem güncellemesi sonrasında aktif hale geleceği ve konu hakkında Kuruma ayrıca bilgi verileceği ve çalışmalar tamamlanıncaya kadar ilgili kişiye ilişkin kayıtların manuel olarak kontrol edilmeye ve gerekirse düzeltilmeye devam edileceği belirtilmiş olup, yazının farklı birçok tarihe ilişkin "Acil Güncelleme Sistemi" ekran görüntülerine yer verildiğinin görüldüğü,

Söz konusu ekran görüntüleri incelendiğinde; ilgili kişiye ait hesap kaydı detaylarının revize edildiği, veri sorumlusundan alınan yazıda bahsedilen sistem geliştirmelerinin tamamlandığı, yapılan geliştirmenin sonuçlarının titizlikle izlendiği ve bu süreçte, ilgili kişiye ilişkin Risk Merkezi bildirimlerinde düzeltme gerektiren bir hususa rastlanmadığı ve yapılan geliştirmenin başarılı olarak sonuçlandığının teyit edildiğinin belirtildiği, bu kapsamda veri sorumlusu tarafından ilgili kişinin Risk Merkezine yanlış aktarılan kişisel verilerinin düzeltilmesi talebinin veri sorumlusu tarafından yerine getirildiği,

Öte yandan, her ne kadar ilgili kişinin yanlış işlenen kişisel verileri veri sorumlusu tarafından ilgili kişinin talebi doğrultusunda düzeltilmiş olsa da başlangıçta gerçeğe aykırı olarak işlenen ve Risk Merkezine aktarılan kişisel veriler bakımından hukuka aykırı bir kişisel veri işleme faaliyetinin gerçekleştirildiği, veri sorumlusu tarafından gerek manuel düzeltmeler yapılması gerek sistemsel iyileştirmelere gidilmesi suretiyle ilgili kişinin talebi yerine getirilmiş olsa dahi, ilgili kişinin veri sorumlusunun bir dönem Kredi Kayıt Bürosuna yaptığı hatalı raporlamalar suretiyle kişisel verilerinin yanlış işlendiği dikkate alındığında veri sorumlusunun kişisel verilerin hukuka aykırı işlenmesini önlemek üzere gerekli idari ve teknik tedbirleri almadığının anlaşıldığı,

Zira, Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere bütün kişisel veri işleme faaliyetleri bakımından riayet edilmesi gerekmekle birlikte, somut olay bakımından veri sorumlusunun işlediği kişisel verilerin doğru ve güncel tutulması bakımından aktif özen yükümlülüğünün bulunduğu,

Bir kişisel veri işleme faaliyetinin hukuka uygunluk arz edebilmesi için gerek Kanun'un 5'inci ve 6'ncı maddesindeki işleme şartlarından birinin varlığı gerek Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere uygunluğun sağlanması gerektiği, somut olay bakımından da, veri sorumlusu tarafından yanlış işlenen kişisel verilerin Risk Merkezine aktarılması sonucunda ortaya çıkan finansal durumdan ötürü ilgili kişinin mağduriyet yaşadığı ve zarara uğratıldığı

değerlendirmelerinden hareketle,

İlgili kişiye ait kişisel veri niteliğini haiz kredi notu bilgisinin veri sorumlusu tarafından yanlış işlenmesi ve Risk Merkezine aktarılmasının Kanun'un 4'üncü maddesinde yer alan genel ilkelerden; "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil ettiği dikkate alındığında, Kanun'un 12'nci maddesinin (1)numaralı fıkrasının (a) bendinde bulunan "...Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek..." yükümlülüğüne aykırı davranan veri sorumlusu hakkında;

Veri sorumlusunun bankacılık sektöründe oldukça büyük bir güce sahip olması,

Veri sorumlusunun oldukça fazla sayıda müşteri ve potansiyel müşteri ile irtibat halinde olması, çeşitlilik arz eden konulara yönelik iletişim kurabilmesi ve bu konularda ilgili kişiler hakkında işlem tesis edebilmesi,

Veri sorumlusunun banka niteliğini haiz olması dolayısıyla, işlediği kişisel veriler üzerinden ilgili kişiler hakkında sonuç elde etmesi ve bu sonuçlar doğrultusunda iş ve eylemlerini gerçekleştirmesi nedeniyle işlenen kişisel veriler bakımından doğruluk ve güncelliğin sağlanması adına aktif özen yükümlülüğünün bulunması,

Veri sorumlusunun işlediği kişisel verileri düzenli ve sistematik olarak Risk Merkezine bildirme yükümlülüğünün bulunması ve bu sisteme bildirilen veriler üzerinden, ilgili kişiler hakkında finansal anlamda önemli sonuçların oluşturulması nedeniyle yanlış bildirilen kişisel verilerin ilgili kişilerin mağduriyetlerine yol açabilmesi

hususları da göz önünde bulundurularak Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 150.000 TL idari para cezası uygulanmasına,

İlgili kişi başvurularına Kanun ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de belirlenen usule uygun ve yeterli bir cevap verilmesi gerektiğinin veri sorumlusuna hatırlatılmasına karar verilmiştir.

KARAR 6:

KIŞISEL VERILERI KORUMA KURUMU

İlgili kişinin kişisel verisinin kamu kurumu personeli olarak görev yapan eski eşi tarafından sorgulanarak elde edilmesi ve adli makamlar ile paylaşılması

(6698 S. K. m. 3, 4, 5, 12, 18)

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Karar Tarihi: 11/03/2021

Karar No: 2021/230

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin kamu kurumu personeli olarak görev yapan, boşanma sürecinde olduğu eşi tarafından görevi kötüye kullanmak suretiyle kendisine erişim yetkisi verilen bir sistem üzerinden, maaş bilgilerinin sorgulandığı, boşanma davasına ilişkin yargılama sürecinde talep edilmemesine rağmen bu bilginin mahkeme ile paylaşıldığı, belirtilen bu program ya da sistemle T.C. kimlik numarası bilinen kişilerin maaşlarının öğrenilmesinin hem 4A/4B bilgisinin kişiselliğine hem de özel şirketlerdeki maaş gizliliğinin ihlaline sebebiyet verdiği hususları ifade edilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

İlgili kişinin şikâyeti hakkında Kurumca başlatılan inceleme çerçevesinde veri sorumlusu kamu kurumunun açıklamalarına başvurulmuş olup, alınan cevabi yazıda özetle;

Konu ile ilgili olarak …. İl Müdürlüğünden bilgi ve belge talep edildiği,

Tabi olunan mevzuat kapsamında, Kurumları ile Sosyal Güvenlik Kurumunun (SGK) görev-yetki alanına giren iş ve işlemlerin ilintili olması nedeniyle tüm personel tarafından ilgili Kurum Portalına erişim sağlanabildiği ve "kontrol arayüzü" üzerinden sınırlı şekilde iş ve işlemler gerçekleştirebildiği,

Bu sınırlı erişim içerisinde kişilerin kimlik numaraları ile çeşitli sorgulamalar yapılabildiğinden, adı geçen personel de dahil olmak üzere tüm personel tarafından hem rutin işler için hem de günlük rutin dışı talepler nedeniyle söz konusu sorgulamanın sürekli yapıldığı,

Öte yandan anılan İl Müdürlüğünce, Kanun ile ilgili Kurumun tüm personelinin defaten bilgilendirildiği ve talimatlandırıldığının bildirildiği,

Şikayete konu veri işleme faaliyetini gerçekleştiren personelin konuya ilişkin açıklamalarının alındığı, yapılan açıklamada söz konusu kişi tarafından rutin işinin bir parçası olarak bahsi geçen sorgulamaları sıkça yaptığı, eşinin memur maaş zammına ilişkin

kendisini haberdar etmesi üzerine ve kendisinin bilgisi dâhilinde bahsi geçen bilgileri sorguladığı, söz konusu zaman diliminde evliliğin aynı çatı altında sürdüğü, Kanunen aynı konutta yaşayanların istisna kapsamında olduğu ve bahsi geçen bilgilerin eşin bilgisi dahilinde sorgulanmasının sakınca teşkil etmediğini düşündüğü, boşanma davasında eşinin iddiasının aksine maaş bilgisinin paylaşılmadığı, bu bilgileri eşi dışında hiç kimse ile paylaşmadığı ve bu hususta mahkemeden bilgi talep edilebileceği ayrıca söz konusu Portaldan sehven kişisel sorgulama yapması hasebiyle Hizmet Merkezlerince "yazılı olarak" uyarıldığının belirtildiği ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/230 sayılı Kararı ile;

Kanunun "Tanımlar" başlıklı 3 üncü maddesinde "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, "veri sorumlusu"nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, "kişisel verilerin işlenmesi"nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

Kanunun, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmü yer almakta olup bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

şeklinde sayıldığı,

Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

Somut olayda veri sorumlusu Kurum bünyesinde, kişilerin kimlik numaraları ile SGK Sorgulaması yapılması kapsamında kişisel verilerin işlenmesinin Kanunun 5 inci maddesinin 2 numaralı fıkrasının (ç) bendine göre veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olduğu, bununla birlikte veri sorumlusunun hizmetlerini elektronik ortamda sürdürmesine ilişkin mevzuatta "Kişisel Verilerin Korunması" başlıklı maddede sistemde yer alan kişisel verilerin kullanılmasında mevzuatta yer alan özel hayatın gizliliğine ilişkin hükümlerin esas alınacağı, ayrıca kullanıcılardan alınan bilgilerin, tanımlanmış hizmetler ve yasal mükellefiyetlerin yerine getirilmesi dışında başka bir amaçla kullanılamayacağının düzenlendiği,

Bu doğrultuda ilgili kişinin kişisel verisinin, kendisi tarafından talep edilmeksizin görev yapan eski eşi tarafından Portal üzerinden sorgulanarak elde edildiği ve söz konusu kişisel verilerin mahkeme ile paylaşıldığı da dikkate alındığında, kişisel veri işleme faaliyetinde kişisel verilerin, hem üçüncü kişilere verildiği hem de görev yetkisi ve tanımlanmış hizmetin dışında bir işleme faaliyetinde işlendiği göz önünde

bulundurulduğunda kişisel verilerin hukuka aykırı işlenmesi ve erişilmesini önlemek ile muhafazasını sağlamak amacıyla veri güvenliğine ilişkin yükümlülüklere uyulmadığı sonucuna varıldığı, değerlendirmelerinden hareketle,

İlgili kişinin kişisel verisinin, veri sorumlusu bünyesinde çalışan bir personel tarafından tanımlanmış hizmetlerin ve yasal mükellefiyetlerin yerine getirilmesi dışında başka bir amaçla kullanılması suretiyle işlenmesinin Kanunun 5 inci maddesinde yer alan işleme şartlarından birine dayanmaması nedeniyle hukuka aykırı olduğu ayrıca Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesi ilkesine aykırı bir veri işleme faaliyetinin gerçekleştiği, bu kapsamda söz konusu faaliyetinin Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği değerlendirildiğinden Kanunun 18 inci maddesinin (3) numaralı fıkrası uyarınca veri sorumlusu bünyesinde görev yapan söz konusu personel hakkında disiplin hükümlerine göre işlem yapılması, öte yandan kişisel verilere erişim yetkisi bulunan personelin söz konusu verilere amacı dışında erişmesinin önlenmesi hususunda 31/05/2018 tarih ve 2018/63 sayılı Kişisel Verileri Koruma Kurulu İlke Kararı da dikkate alınarak gerekli tedbirlerin alınması ve yapılacak işlemlerin sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

KARAR 7:

KIŞISEL VERILERI KORUMA KURUMU
Bir hastanenin veri ihlali bildirimi
(6698 S. K. m. 12, 18)

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Karar Tarihi: 20/04/2021
Karar No: 2020/407
Konu Özeti: Bir hastanenin veri ihlali bildirimi

Veri sorumlusu bir hastane tarafından Kuruma intikal ettirilen veri ihlal bildiriminde;

Veri ihlalinin; hastanede çalışan hekimin hastalarına ait dosyaların arşivden alınarak kendisinin talimatıyla bazı hastane çalışanları aracılığıyla hastane dışına çıkarılmasıyla gerçekleştiği,

Veri ihlalinin; dosyaları hastane dışına çıkarmaya teşebbüs eden bir çalışanın görülmesinden 17 gün sonra kamera kayıtlarının incelenmesi neticesinde tam olarak tespit edildiği,

İhlalden; 789 hastanın etkilendiği,

İhlalden; kimlik, iletişim, sağlık bilgileri ve genetik verilerin hasta kartında yer alan bilgiler (T.C Kimlik numarası, adı, soyadı, baba adı, ana adı, sosyal güvenlik numarası, özel sigorta, anlaşmalı kurum, çalıştığı kurum, uyruğu, doğum tarihi, cinsiyet, medeni hali, kan grubu, mesleği, vergi dairesi, vergi numarası, adres, posta kodu, e-posta, ev telefonu, iş telefonu, cep telefonu, son randevu cep ve ev telefonu, sigortalı durumu, emekli olup olmadığı, poliçe no, engel durumu, çalışan adı, tedavi olunan doktorlar ve branşlar gibi bilgiler) ile hasta dosyası anamnez içeriğinin (kullandığı ilaçlar, alışkanlıklar, alerjik öyküsü, soygeçmiş, psikolojik durum, bulgular, laboratuvar tetkikleri, öntanı, tanı, tedavi ve bakım planı, geçirmiş olunan hastalıklar, ameliyatlar vb. bilgiler) etkilendiği ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Kararı ile,

İhlalden 789 hastanın etkilendiği ancak karakol tutanağına göre tespit edilen 54 adet hasta dosyasının geri alınarak yedieminliğe teslim edildiği, geri kalan dosyaların akıbetinin ise bilinmediği dikkate alındığından hasta dosyalarının kaybolması durumunun önlenemediği ve bu durumun söz konusu hasta dosyalarının kaybolmasına yönelik risklerin azaltılmasına dair yeterli tedbirlerin alınmadığını gösterdiği,

İhlalden; kimlik, iletişim, lokasyon, özlük, genetik veri, sağlık verileri gibi veri kategorilerine ait çok sayıda kişisel verinin ve özel nitelikli kişisel verinin etkilenmiş olduğu

hususunun ilgili kişilerin ihlal sebebiyle önemli olumsuz etkilere maruz kalmaları olasılığının bulunduğunun göstergesi olduğu,

İhlal ile ilgili olan çalışanların, sağlık verileri ve genetik veriler de dahil olmak üzere özel nitelikli çok sayıda kişisel verinin işlenme sürecinde yer aldığı göz önünde bulundurulduğunda; veri sorumlusu tarafından çalışanlara tanımlanan kişisel verilerin korunması eğitiminin tamamlanmasının sağlanmadığı, eski çalışanın kişisel verilerin korunması ile ilgili eğitim almış olmasına rağmen arşiv odasındaki belgelerin taşınmasına yardım ettiğinin anlaşıldığı dikkate alındığında Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan "Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,…gerekir." ifadesine aykırı olarak veri sorumlusu tarafından çalışanlara kişisel verilerin korunmasına yönelik yeterli eğitimin verilmediğinin göstergesi olduğu,

İhlal şüphesini doğuran olayların bulunmasına rağmen; ihlalin 17 gün sonra tespit edilmesinin veri sorumlusu tarafından kişisel veri güvenliği politika ve prosedürlerinin iyi bir şekilde hazırlanmadığı veya takip edilmediği, ayrıca bu durumun alınan mevcut güvenlik önlemlerinin etkili kullanılamadığı hususlarının göstergesi olduğu,

İhlali gerçekleştiren ve diğer çalışanların Başhekimliğin izni ve onayı bulunmaksızın, eski çalışanın ve aynı yerde yer alan bir şirket çalışanının arşiv odasına girebildiği ve hasta dosyalarını dışarı çıkarabildiği, ayrıca söz konusu durumun kamera kayıtlarında görülmesine rağmen 1 ayı aşkın süre boyunca ihlalin devam ettiği ve kamera kayıtlarının ancak ihlal anlaşıldıktan sonra kontrol edildiği hususunun Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan "… Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi…gerekir." ifadesine aykırı olarak kamera kayıtlarının kontrolünün ve hastalara ait kayıtların tutulduğu arşiv odasına yetkili olmayan kişilerin girmemesini sağlayacak yeterli idari tedbirlerin alınmadığını gösterdiği,

İhlalin gerçekleşmesinden önce, Kişisel Verileri Koruma ve Bilgi Güvenliği Kurulu oluşturulmasına, Veri İhlali Müdahale Planı hazırlanmasına ve KVKK kapsamında ilgili kişilerden veya kurumlardan gelecek talepleri karşılamak üzere algoritma oluşturulmasına rağmen; yedieminliğe teslim edilen hasta dosyalarının hastane arşivindekilerden daha fazla veri içerdiğinin ihlalden sonra tespit edildiği hususlarının Kişisel Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi" başlığı altında yer alan "Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılamadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır." ifadelerinde yer aldığı üzere; veri sorumlusu tarafından alınan mevcut güvenlik önlemlerinin iyi bir şekilde hazırlanmaması veya kullanamaması nedeniyle ihlalin tespit edilmesi ve önlenmesine yönelik tedbirlerin zamanında ve yeterli ölçüde alınamadığı,

İzinsiz olarak hastaneden çıkarılan birçok hasta dosyasının akıbetinin halen bilinmemesinin "Kişisel Veri Güvenliği Rehberi"nin "Mevcut Risk ve Tehditlerin Belirlenmesi" başlığı altında yer alan "Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; Kişisel verilerin özel nitelikli kişisel veri olup olmadığı, Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır …" ifadelerine aykırı olarak hasta dosyalarının kaybolması durumunun önlenemediği veya kaybolması halinde risklerin azaltılmasına dair yeterli tedbir alınmadığını gösterdiği,

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL,

- İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği,
- İlgili kişilerden hastaneye gelen bir kişi dışında, hiç birine ihlalin bildirilmemiş olduğu,

hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası hükmü ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına yönelik ifadeleri çerçevesinde bildirim yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL olmak üzere toplam 600.000 TL idari para cezası uygulanmasına,

İlgili kişilere Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan hususları içeren bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

KARAR 8:

KIŞISEL VERILERI KORUMA KURUMU

Bir bilişim şirketinin kişisel veri ihlali bildirimi

(6698 S. K. m. 4, 12, 18)

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Karar Tarihi: 12/03/2020

Karar No: 2020/216

Konu Özeti: Bir bilişim şirketinin kişisel veri ihlali bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

Veri sorumlusu Şirketin sistemlerine siber saldırı gerçekleştirilerek sistemlerinde yer alan verilerin elde edilmeye çalışıldığı,

Pilot adı verilen uygulamada debugging özelliğinin açık olduğu ve şirket için sistem geliştirmesi yapan geliştiricilerin bu özelliği kullanarak uygulamadaki hataları tespit ettiği ve iyileştirme gerçekleştirdiği,

İhlale konu siber saldırı ile Pilot uygulamasına internet üzerinden erişim sağlamaya çalışan kişinin(lerin), uygulamaya daha önce giriş yapmış kişilere ait "PHPSESSID" değerini elde ettiği ve Pilot uygulamasına erişim sağladığı,

Debugging özelliğinin açık olmasının sebebinin sisteme internet üzerinden erişilerek geliştirmelerin yapılmasına olanak sağlamak olduğu, ancak bu durumun internet üzerinden siber saldırılar gerçekleştirilerek sisteme erişilmesine olanak tanıdığı,

Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilemediği ancak veri sorumlusunun sistemlerinde yer alan verilerin tümü dikkate alındığında sistemde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği,

İlgili kişilere ilişkin sistemde yer alan kayıtların 1259 sözleşme, 701 alan adı başvuru dosyası (içerisinde imza sirküleri, vergi levhası ve kişi kimlik fotokopisi kayıtları) olduğu,

Sistemde ayrıca elli bin kredi kartı bilgisi yer aldığı, ancak bu kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece sekiz bin kartın aktif olduğunun tespit edildiği,

İhlalden etkilenen kişi kategorilerinin müşteriler ve potansiyel müşteriler olduğu,

Saldırganların hangi verilere eriştiklerinin tespit edilemediği, sistemde yer alan verilerin kimlik, iletişim, işlem güvenliği (kullanıcı adı ve parola bilgileri), ödeme Bilgileri (kredi kartı numarası) olduğu,

Ele geçirilen kredi kartı bilgilerinin 2018 tarihi öncesinde veri sorumlusu Şirkete aktarılan bilgiler olduğu, 2016 tarihi itibari ile ödeme hizmetlerinde iyileştirme çalışmaları

kapsamında bir proje başlatıldığı, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplanmakta ve onlar tarafından saklanmakt, ancak tüzel kişi müşterilerin imza sirkülerinin ekinde yer alan eski kimlik fotokopilerinde kan grubu ve din bilgisi hanelerinin bulunduğu ve bazı imza sirkülerinde kimlik fotokopisinin arka yüzünün de yer alabildiği dikkate alınarak; bazı müşteriler için saldırganların bu verilere de erişme ihtimali olabileceği,

Sistemde yer alan tüm kayıtların incelendiği ve sayımlarda (imza sirkülerlerinde yer alan kimlik fotokopileri de dahil) 1.784 adet eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğunun tespit edildiği,

İhlalden etkilenen tüm müşterilere e-posta göndermek suretiyle bildirimde bulunulduğu, bir kısım müşterilere mümkün olduğunca telefonla da bilgilendirme gerçekleştirildiği,

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 12/03/2020 tarih ve 2020/216 sayılı sayılı Kararı ile;

Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilememesinin, veri sorumlusu tarafından sızma veya herhangi bir anomali olup olmadığının belirlenmesi noktasında kontrol ve uyarı mekanizmalarının etkin bir şekilde kullanılmadığının göstergesi olduğu,

Veri sorumlusu tarafından hangi kişisel verilerin etkilendiğinin tespit edilemediği ancak sistemlerde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği, bu kişilerden 1.784 tanesinin eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğu ayrıca elli bin kredi kartı bilgisi yer aldığı,

Veri sorumlusunun kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece sekiz bin kartın aktif olduğu, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplandığı ve onlar tarafından saklandığı bu çerçevede veri sorumlusunun ödeme sistemini değiştirmiş olmasına rağmen sistemde bulunan kredi kartı bilgilerini imha etmeyerek 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 4 üncü maddesinin (2) numaralı fıkrasının (b) ve (ç) bendine aykırı hareket ettiği,

Şirket dışından erişim için güvenlik amacıyla VPN ile Şirket IP'sine bağlanıldığı ve kişilere özel kullanıcı adı ve VPN şifresi verildiği, saldırganların da sisteme SFTP ve VPN aracılığı ile bağlandığı, ihlalden sonra 29.01.2020 tarihinde yapılan ve veri sorumlusu tarafından Kurumumuza gönderilen sızma testinde özellikle web uygulamalarında yüksek ve orta seviyede açıklıkların tespit edildiği göz önüne alındığında bu durumun veri sorumlusu tarafından gerekli teknik tedbirlerin alınmadığının göstergesi olduğu,

Veri sorumlusunun https://www.****.com.tr adresinde domain ve hosting hizmetlerinin satın alındığı ekranları incelendiğinde satın alma süreçlerinde kimlik ve iletişim bilgilerinin talep edildiği ancak herhangi bir aydınlatma metninin bulunmadığı göz önüne alındığında veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında yükümlülüklerini yeterli seviyede yerine getirmediği kanaatine varıldığı,

Veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (çift faktör özelliği olan sistemlerde bu özelliğin aktifleştirilmesi, VPN erişimde kullanılan sertifikaların yenilenmesi, çalışanlarının e-posta erişimlerinin iki aşamalı kimlik doğrulama olarak güncellenmesi, log kayıtlarının adli olaylarda kanıt niteliğinde kullanılabilmesi için zaman damgasıyla damgalanması, logların korelasyonunun sağlanması vb) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduğu değerlendirmelerinden hareketle, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL idari para cezasının uygulanmasına,

Veri ihlalinin 09.10.2019 tarihinde 14:04'de gerçekleştiği, 11.10.2019 tarihinde saat 14.04'de veri sorumlusu tarafından tespit edildiği, 14.10.2019 tarihinde Kurula 72 saat içinde bildirildiği dikkate alındığında bu hususta yapılacak bir işlem bulunmadığına karar verilmiştir.

KARAR 9:

KIŞISEL VERILERI KORUMA KURUMU
Bir bankanın veri ihlal bildirimi hakkında
(6698 S. K. m. 12, 18)

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Karar Tarihi: 29/09/2020
Karar No: 2020/744
Konu Özeti: Bir bankanın veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

Veri ihlalinin, Bankanın Veri Sızıntısı ekibi tarafından Teftiş Kurulu Başkanlığı'na iletilen bildirime istinaden soruşturma çalışmalarına başlanılarak tespit edildiği,

Çalışanın veri sorumlusu nezdinde kullandığı e-posta adresine gelen ve ilgili adresten iletilen e-postalara ilişkin kayıtların incelenmesi neticesinde çalışanın 346 müşteriye ait bilgileri bir word dokümanına işlediği ve söz konusu dokümanı e-posta ile bir yatırım firmasında çalıştığını ve arkadaşı olduğunu iddia ettiği 3. kişiye gönderdiği,

Söz konusu müşterilerin hepsinin bir yatırım şirketine para transferlerinin bulunduğu,

İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem ve finans verileri olduğu,

Verileri paylaşılan müşterilerin ihlale sebebiyet veren çalışanın ilişkili olduğu şubenin müşterileri olmadığı, bu nedenle çalışanın verileri toplaması ve paylaşmasının mesnedinin bulunmadığı ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 29/09/2020 tarih ve 2020/744 sayılı Kararı ile,

İhlalden 346 Banka müşterisinin şube no, hesap no, ad-soyadı, cep telefonu numarası ve bu müşterilerin Bankadaki hesaplarından bir yatırım firması hesabına gönderdikleri yatırım işlemi tutar bilgilerinin etkilendiği,

İhlal ile ilgili olan personelin veri ihlalinin gerçekleşmesinden 1 seneyi aşkın süre önce 09.10.2018 tarihinde "Kişisel Verilerin Korunması Kanunu" eğitimini tamamlamış olmasına rağmen, bahse konu eğitimden sonra bizzat ihlali gerçekleştirmiş olmasının verilen eğitimin yeterli ve etkin olmadığı hususunda şüphe oluşturduğu,

Banka dışına giden e-postalara ilişkin Veri Sızıntısı Tespit/Önleme Sisteminin mevcut olduğunun belirtilmesine rağmen söz konusu ihlale neden olan e-postanın DLP sistemleri tarafından engellenmemesi ve ihlale sebep olan çalışanın kişisel verilerin aktarımı gerçekleştirilebildiği dikkate alındığında, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde "Mevcut Risk ve Tehditlerin Belirlenmesi" başlığı altında yer alan "Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; - Kişisel verilerin özel nitelikli kişisel veri olup olmadığı, - Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, - Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.", ifadeleri uyarınca yetkisiz olarak kişisel veri aktarımı önleme açısından veri sorumlusunun almış olduğu tedbirlerin yetersiz kaldığı,

Banka tarafından alınan idari ve teknik tedbirlere rağmen Banka personelinin 346 müşteriye ait kişisel verileri, işlenme amacı dışında üçüncü taraflara iletebildiği ve bu durumun, Kişisel Verileri Koruma Kurulu'nun 31/05/2018 tarih ve 2018/63 sayılı ilke kararında "…Bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698

sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği…" ifadelerine aykırı olarak veri güvenliğini sağlamaya yönelik veri sorumlusunun almış olduğu teknik ve idari tedbirlerin yetersiz kaldığının göstergesi olduğu dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 225.000 TL,

İlgili kişilere gerekli bildirimlerin yapıldığı ve söz konusu bildirim örneklerinin tarafımıza gönderildiği,

Ancak, ihlalin 31.10.2019 tarihinde gerçekleştiği ve Bankanın Teknoloji Veri Sızıntısı ekibi tarafından 04.11.2019 tarihinde Teftiş Kurulu Başkanlığı'na iletildiği, veri sorumlusunun Kurumumuza bildirimi 06.12.2019 tarihinde gerçekleştirdiği dikkate alındığında Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirim koşulunun sağlanmadığı,

dikkate alındığında, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket etmesi nedeniyle veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL olmak üzere toplam 275.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARAR 10 :

KIŞISEL VERILERI KORUMA KURUMU

Bir internet servis sağlayıcısının veri ihlali hakkında karar

(6698 S. K. m. 12, 18)

*** İncelemekte olduğunuz karar www.kvkk.gov.tr adresinden "Kurul Karar Özetleri" bölümünden alınmıştır.

Karar Tarihi: 12/03/2020

Karar No: 2020/213

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

Şirketin müşterilerinin paket değişikliği, fatura ödeme, arıza bildirimi gibi abonelik işlemlerini yapmalarına olanak sağlayan ve kendilerine tanımlanan kullanıcı adı ve şifre ile giriş yapabildikleri bir Online İşlem Merkezi bulunduğu,

Şirketin fatura ödeme sisteminde online (çevrimiçi) işlemlerde fatura ödemesi yapılamadığı ve sorunun Şirkete müşteriler tarafından bildirildiği,

Müşterinin ödeme yaptığı sırada ekranda "fatura seçilmesi gerektiği" uyarısı belirdiği,

Sorun giderilmek üzere çalışma yapılırken bir güvenlik açığının ortaya çıktığı,

Güvenlik açığı sebebiyle müşterilerin kredi kartı bilgilerinin üçüncü taraflarca görüntülendiği,

İhlalin kök nedeninin uygulamaya bilgi kaydı (log) üreten özelliklerin eklenerek "debug" ile düzeltilmesi girişiminin olduğu,

69 kişiye ait kart bilgisinin 649 adet Şirket müşterisi tarafından görüntülendiğinin tespit edildiği, ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 12.03.2020 tarih ve 2020/213 sayılı Kararı ile;

Yazılım geliştiricilere sözlü olarak aktarılmış olan değişiklik talebinin test ortamında değil de gerçek ortamda yapılmasının, uygulamada yapılan değişikliklerin canlıya (gerçek/çalışır ortam) alma süreçleri ile ilgili prosedürlerin uygulanmadığının göstergesi olduğu bu durumun ise teknik ve idari tedbir eksikliği olduğu,

Test süreçlerinin yetersizliği veri sorumlusunun kendisi tarafından belirtilmiş olup bu durumun uygulama güvenliği açısından veri sorumlusunun gerekli teknik ve idari tedbirleri almadığının göstergesi olduğu,

Sistem ara yüzlerinde kişisel verilerin ya hiç gösterilmediğinin ya da maskelendiğinin şirket tarafından belirtilmiş olmasına rağmen müşterilere ait kimlik ve finans verilerinin yapılan hata sonucunda görüntülenebilmesinin teknik bir eksiklik olduğu,

Veri sorumlusunun bir veri güvenliği politikasının bulunduğu ancak bu politikanın yürürlük tarihinin veri ihlalinin gerçekleştiği tarihten sonra olduğu dikkate alınarak, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL idari para cezasının uygulanmasına karar verilmiştir.

KARAR 11:

KIŞISEL VERILERI KORUMA KURUMU

Kişisel verilerin sorgulanmasına imkan tanıyan yazılım/ program/uygulamaları – Durumun veri sorumlularının veri güvenliğine ilişkin yükümlülüklerini düzenleyen hükümlerine aykırılık oluşturduğu – Veri güvenliği ihlallerinin önüne geçilmesi için yapılacaklar

(6698 S. K. m. 12, 15, 18) (5271 S. K. m. 158)

RGT: 21.11.2019

RG NO: 30955

Karar Tarihi: 18/10/2019

Karar No: 2019/308

Kişisel Verileri Koruma Kurumuna intikal eden ihbarlar kapsamında avukatlar/hukuk büroları ile finans, gayrimenkul danışmanlık, sigorta vb. sektörlerde faaliyet gösteren bazı kişi ve kuruluşlar tarafından muhtelif yollarla elde edilen veriler üzerinden vatandaşların kimlik ve iletişim bilgileri gibi kişisel verilerinin sorgulanmasına imkân tanıyan yazılım/program/uygulamaların kullanılmakta olduğu tespit edilmiştir. Yapılan değerlendirme sonucunda bu durumun, 6698 sayılı Kişisel Verilerin Korunması Kanununun veri sorumlularının veri güvenliğine ilişkin yükümlülüklerini düzenleyen 12 nci maddesi hükümlerine aykırılık oluşturduğu dikkate alınarak, yaşanabilecek veri güvenliği ihlallerinin önüne geçilmesini teminen;

- Bu mahiyetteki yazılımları/programları/uygulamaları kullandığı tespit edilenler hakkında Türk Ceza Kanunu kapsamında gerekli adli işlemlerin tesisi için konunun, 5271 sayılı Ceza Muhakemesi Kanununun 158 inci maddesi hükmü uyarınca ihbaren ilgili Cumhuriyet Başsavcılıklarına bildirileceği,
- Kişisel Verileri Koruma Kurulunun görev alanına giren yönüyle de veri sorumluları hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 18 inci maddesi hükmü çerçevesinde idari işlem tesis edileceği hususlarında kamuoyunun bilgilendirilmesine,
- 6698 sayılı Kişisel Verilerin Korunması Kanununun 15 inci maddesinin altıncı fıkrası hükmü uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına oybirliği ile karar verilmiştir.

4.4. Bilişim Suçları ile Mücadele Stratejileri ve Alınması Gereken Önlemler

Teknolojinin hızlı gelişimi ve dijitalleşmenin yaygınlaşması, bilişim suçlarının artmasına ve daha karmaşık hale gelmesine yol açmıştır. Bu durum, bilişim suçlarıyla mücadeleyi hem hukuki hem de teknik açıdan zorunlu ve öncelikli hale getirmiştir. Literatürde bilişim suçlarıyla mücadele, kapsamlı stratejiler ve çok katmanlı önlemler gerektiren dinamik bir alan olarak ele alınmaktadır (Kara, 2020: 67). Türkiye ve dünya genelinde bilişim suçlarına karşı uygulanan stratejiler; yasal düzenlemeler, teknik altyapı

güçlendirmeleri, farkındalık artırma çalışmaları ve uluslararası işbirliği gibi temel unsurları içermektedir (Demirtaş ve Arslan, 2021: 120).

Öncelikle, bilişim suçlarıyla mücadelede hukuki altyapının güçlendirilmesi gerekliliği vurgulanmaktadır. Türkiye'de 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile TCK'nın bilişim suçları ile ilgili maddeleri önemli yasal dayanaklardır (Aksoy, 2019: 89). Ancak, teknolojide yaşanan hızlı değişimler karşısında mevcut mevzuatın yetersiz kalabildiği ve düzenlemelerin zamanında güncellenmesinin kritik olduğu literatürde sıkça belirtilmektedir (Yılmaz, 2020: 54). Özellikle siber suçların uluslararası boyut kazanması sebebiyle, Türkiye'nin de uluslararası standartlara uyumlu mevzuat geliştirmesi zorunludur (Özkan ve Demir, 2022: 103).

Teknik alanda, bilişim suçlarıyla mücadelede etkin adli bilişim ve siber güvenlik altyapısının oluşturulması büyük önem taşımaktadır. Adli bilişim, suçun işlenme yöntemlerinin tespiti, delillerin toplanması ve analizinde kritik bir rol oynamaktadır (Şahin ve Güngör, 2021: 74). Türkiye'de adli bilişim kapasitesinin artırılması ve bu alanda uzmanlaşmış personel sayısının çoğaltılması gerekmektedir (Çelik, 2021: 112). Ayrıca, kamu kurumları, özel sektör ve vatandaşlar düzeyinde güçlü siber güvenlik önlemleri alınmalı, güncel antivirüs programları, güvenlik duvarları ve saldırı tespit sistemleri yaygınlaştırılmalıdır (Erdoğan, 2020: 59).

Bilişim suçlarının önlenmesinde eğitim ve farkındalık çalışmalarının önemi de büyüktür. Toplumun bilişim suçlarının riskleri ve alınması gereken önlemler hakkında bilinçlendirilmesi, suçun işlenme oranını azaltmada etkili bir yöntemdir (Kaya ve Demirtaş, 2022: 95). Okullarda ve işyerlerinde siber güvenlik eğitimlerinin yaygınlaştırılması, bireylerin şüpheli faaliyetlere karşı dikkatli olmalarını sağlar (Demir ve Yalçın, 2020: 118). Ayrıca, kurumların siber güvenlik politikaları oluşturması ve düzenli olarak güncellemesi gerekmektedir (Öztürk, 2021: 84).

Uluslararası işbirliği, bilişim suçlarının sınırları aşan doğası nedeniyle mücadelede vazgeçilmez bir stratejidir. Türkiye, uluslararası hukuk çerçevesinde siber suçlarla mücadele eden çeşitli anlaşmalara taraf olmuştur (Kara, 2020: 70). Bu işbirliği, bilgi paylaşımı, ortak operasyonlar ve suçluların iadesi gibi konularda etkili olmaktadır (Çelik ve Yılmaz, 2021: 138). Ancak, uluslararası koordinasyonun daha etkin hale

getirilmesi ve siber suçlarla mücadelede ortak standartların belirlenmesi için çalışmalar sürdürülmelidir (Özkan ve Demir, 2022: 110).

Hukuki, teknik, eğitim ve uluslararası boyutların yanında, bilişim suçlarıyla mücadelede kamu ve özel sektör işbirliği de kritik önem taşımaktadır. Siber güvenlik alanında faaliyet gösteren özel firmalarla devlet kurumlarının ortak hareket etmesi, daha kapsamlı ve hızlı müdahalelere olanak tanır (Erdoğan, 2020: 62). Bu işbirliği kapsamında, kritik altyapıların korunması, siber saldırıların önceden tespiti ve olay müdahalesi gibi faaliyetler ortaklaşa yürütülmektedir (Kaya ve Demirtaş, 2022: 98).

Bireylerin de bu mücadelede rol alması gerekmektedir. Kişisel verilerin korunması ve güvenliğinin sağlanması, bireysel düzeyde dikkatli davranmayı ve temel siber güvenlik tedbirlerinin alınmasını gerektirir (Demirtaş, 2020: 76). Şifre güvenliği, güncel yazılım kullanımı ve şüpheli e-postalara karşı dikkatli olma gibi önlemler, bilişim suçlarının önlenmesine katkı sağlar (Demir ve Yalçın, 2020: 115).

Özetle, bilişim suçlarıyla mücadele stratejileri çok boyutlu ve koordineli bir yaklaşım gerektirmektedir. Hukuki düzenlemelerin güncellenmesi, teknik altyapının güçlendirilmesi, eğitim ve farkındalık çalışmaları, uluslararası işbirliği ve kamu-özel sektör işbirliği bu stratejinin temel bileşenleridir. Bu alanlarda yapılacak iyileştirmeler, bilişim suçlarıyla mücadelede etkinliği artıracak ve toplumun dijital güvenliğini sağlamada kritik rol oynayacaktır (Çelik ve Yılmaz, 2021: 140).

4.4.1. Kişilerin Ya Da Kurumların Alması Gereken Önlemler

Bilişim teknolojilerinin hızla gelişmesi ve dijitalleşmenin yaygınlaşması, kişilerin ve kurumların siber güvenlik alanında daha dikkatli ve bilinçli hareket etmelerini zorunlu kılmıştır. Artan bilişim suçları ve siber tehditler, bireysel ve kurumsal düzeyde etkili önlemlerin alınmasını gerektirmektedir (Demir ve Yalçın, 2020: 115). Literatürde, siber güvenlik alanında alınması gereken önlemler temel olarak teknik, hukuki ve eğitsel kategoriler altında incelenmektedir (Kaya ve Demirtaş, 2022: 92).

4.4.1.1. Teknik Önlemler

Teknik önlemler, kişisel ve kurumsal bilgi sistemlerinin güvenliğinin sağlanması için atılan en önemli adımlardır. Bu önlemler arasında, güncel ve güçlü şifre kullanımı, çok faktörlü kimlik doğrulama, düzenli yazılım güncellemeleri ve güvenlik duvarlarının

etkin kullanımı yer almaktadır (Öztürk, 2021: 82). Şifrelerin karmaşık, benzersiz ve düzenli olarak değiştirilmesi, hesapların yetkisiz erişimlere karşı korunmasında temel bir yöntemdir (Demirtaş, 2020: 74). Ayrıca, kurumlar, kritik sistemlerini dış saldırılara karşı korumak amacıyla antivirüs yazılımları, saldırı tespit ve önleme sistemleri (IDS/IPS) gibi teknolojileri kullanmalıdır (Erdoğan, 2020: 60).

Veri yedekleme stratejileri de teknik önlemler arasında kritik bir yer tutmaktadır. Kurumların, veri kaybı ve fidye yazılımı gibi tehditlere karşı düzenli ve güvenli yedekleme yapması, olası saldırılarda iş sürekliliğini sağlamaya yardımcı olur (Kara, 2020: 68). Ayrıca, güvenli veri iletimi için şifreleme yöntemlerinin kullanılması, verilerin üçüncü şahıslar tarafından ele geçirilmesini engellemektedir (Aksoy, 2019: 90).

4.4.1.2. Hukuki Önlemler

Hukuki önlemler, bireylerin ve kurumların dijital ortamda hak ve sorumluluklarının belirlenmesi açısından önemlidir. Türkiye'de kişisel verilerin korunması kapsamında yürürlüğe giren 6698 sayılı KVKK, kurumların veri işleme süreçlerinde uyulması gereken kuralları ortaya koymaktadır (Demirtaş, 2020: 75). Kurumlar, KVKK çerçevesinde kişisel verilerin güvenliğini sağlamak, veri ihlallerini önlemek ve gerektiğinde ilgili mercilere bildirimde bulunmakla yükümlüdür (Özkan ve Demir, 2022: 105).

Hukuki düzenlemeler aynı zamanda kurumların siber güvenlik politikaları oluşturmasını da zorunlu kılmaktadır. Bu politikalar, kurum içi sorumlulukları belirlemek, siber saldırı durumlarında uygulanacak prosedürleri düzenlemek ve çalışanların bilinçlendirilmesini sağlamak açısından kritik öneme sahiptir (Çelik ve Yılmaz, 2021: 135). Bireyler ise hukuki hakları konusunda bilinçlenmeli ve dijital ortamlarda haklarını koruyacak bilgi ve donanıma sahip olmalıdır (Demir ve Yalçın, 2020: 120).

4.4.1.3. Eğitsel Önlemler

Eğitim ve farkındalık, bilişim güvenliğinin en etkili araçlarından biridir. Bireylerin ve kurum çalışanlarının siber tehditlere karşı bilinçlendirilmesi, insan kaynaklı güvenlik açıklarının azaltılmasında temel strateji olarak öne çıkmaktadır (Kaya ve Demirtaş, 2022: 95). Özellikle sosyal mühendislik saldırıları, phishing (oltalama)

yöntemleri ve zararlı yazılımlar konusunda yapılan eğitimler, kullanıcıların saldırılara karşı daha hazırlıklı olmasını sağlar (Demirtaş ve Arslan, 2021: 118).

Kurumlar, düzenli aralıklarla siber güvenlik eğitimleri düzenlemeli, güncel tehditler ve alınması gereken önlemler hakkında personelini bilgilendirmelidir (Erdoğan, 2020: 63). Eğitim programları, çalışanların güvenlik politikalarına uyum sağlamasını, güvenlik açıklarının erken tespit edilmesini ve olası saldırılara karşı hızlı reaksiyon göstermesini mümkün kılar (Şahin ve Güngör, 2021: 76). Ayrıca, okullarda verilen temel dijital okuryazarlık ve siber güvenlik eğitimleri de geleceğin güvenlik bilincine sahip bireylerinin yetişmesine katkı sunmaktadır (Kara, 2020: 70).

4.4.2. Kurumsal Güvenlik Politikaları ve Yönetim

Kurumların etkili siber güvenlik önlemleri alabilmesi için, kurumsal düzeyde kapsamlı güvenlik politikaları geliştirmesi gerekmektedir. Bu politikalar, kurumun ihtiyaçlarına uygun risk değerlendirmeleri yapmayı, güvenlik standartlarını belirlemeyi ve güvenlik ihlallerine karşı acil müdahale planları oluşturmayı içermelidir (Çelik, 2021:. 115). Ayrıca, bilgi güvenliği yönetim sistemlerinin (BGYS) uygulanması, kurumların bilgi varlıklarını sistematik olarak korumasını sağlar (Özkan ve Demir, 2022: 108).

Kurumsal yapı içerisinde siber güvenlik birimleri kurulmalı ve bu birimler, sistemlerin 7/24 izlenmesini, saldırı tespitini ve müdahalesini gerçekleştirmelidir (Erdoğan, 2020: 60). Ayrıca, kurum içi iletişim kanalları üzerinden düzenli olarak güvenlik uyarıları yapılmalı ve güvenlik kültürü desteklenmelidir (Demir ve Yalçın, 2020: 121).

4.4.3. Bireysel Önlemler ve Dijital Haklar

Bireylerin alacağı önlemler de dijital güvenlik açısından büyük önem taşımaktadır. İnternet kullanıcıları, kişisel bilgilerini paylaşırken dikkatli olmalı, güvenilir olmayan kaynaklardan gelen bağlantılara tıklamamalıdır (Demirtaş, 2020: 78). Güvenlik yazılımlarının düzenli güncellenmesi, güçlü parola kullanımı ve iki faktörlü kimlik doğrulama yöntemlerinin tercih edilmesi, bireysel siber güvenliği artıran basit fakat etkili adımlardır (Öztürk, 2021: 85).

Ayrıca, bireylerin dijital haklarını bilmeleri ve bu hakları korumaları gerekmektedir. Kişisel verilerin korunması konusunda yasal haklar, veri sahiplerinin

taleplerini iletmeleri ve ihlaller durumunda yasal yollara başvurmaları açısından kritik öneme sahiptir (Kara, 2020: 72). Bireysel farkındalık arttıkça, kişisel ve toplumsal güvenlik de güçlenecektir (Demir ve Yalçın, 2020: 122).

4.4.4. Devletlerin Alması Gereken Önlemler

Bilişim teknolojilerinin hızla gelişmesiyle birlikte, devletler dijital çağın getirdiği yeni tehditlere karşı etkin ve kapsamlı önlemler almak zorundadır. Siber suçların sınır tanımayan yapısı, devletlerin ulusal güvenlik, kamu düzeni ve ekonomik istikrar açısından siber güvenliği stratejik bir öncelik haline getirmesine neden olmuştur (Demirtaş, 2020: 75). Devletlerin bu alandaki sorumlulukları hukuki, teknik, eğitimsel ve uluslararası işbirliği boyutlarında kendini göstermektedir. İlk olarak, hukuki altyapının güçlendirilmesi büyük önem taşımaktadır. Türkiye'de 5651 sayılı İnternet Kanunu ve 6698 sayılı KVKK gibi düzenlemeler, bilişim suçlarına karşı temel hukuki çerçeveyi oluşturmasına rağmen, teknolojinin hızla gelişmesiyle mevzuatın güncel kalması gerekmektedir (Aksoy, 2019: 87). Devletler, ceza hukuku ve bilişim hukuku alanlarında uluslararası standartlara uyum sağlayarak, siber suçlulara karşı daha etkin bir mücadele imkanı yaratmalıdır (Özkan ve Demir, 2022: 104). Bu bağlamda, sadece suçları tanımlamakla kalmayıp, suç işlendikten sonra faillerin tespiti ve yargılanması için gerekli mekanizmaların oluşturulması da gerekmektedir.

Teknik altyapının güçlendirilmesi ise devletlerin alması gereken bir diğer kritik önlemdir. Siber saldırılar özellikle kritik altyapılar üzerinde yoğunlaşmaktadır. Enerji, finans ve sağlık gibi hayati öneme sahip sistemlerin korunması devletin asli görevleri arasında yer alır (Erdoğan, 2020: 58). Ulusal siber savunma merkezleri kurulmalı, gelişmiş saldırı tespit ve müdahale sistemleri devreye sokulmalıdır. Ayrıca, kamu kurumlarının bilgi teknolojileri altyapısının sürekli olarak güncellenmesi, güvenlik açıklarının kapatılması devletin teknik sorumluluğudur (Şahin ve Güngör, 2021: 73). Devletler, siber güvenlikte dışa bağımlılığı azaltmak için yerli teknolojilerin geliştirilmesini desteklemeli, Ar-Ge faaliyetlerine kaynak ayırmalıdır (Kaya ve Demirtaş, 2022: 93). Bu yaklaşım, sadece teknolojik altyapının güvenliğini artırmakla kalmaz, aynı zamanda ekonomik ve stratejik bağımsızlığı da güçlendirir.

Eğitim ve farkındalık programları da devletlerin alması gereken önemli önlemler arasında yer almaktadır. Siber tehditlerin sürekli değişen yapısı, halkın ve kamu

personelinin bilinçlendirilmesini zorunlu kılar (Demir ve Yalçın, 2020: 119). Özellikle kamu kurumlarında çalışanların düzenli olarak siber güvenlik eğitimleri alması, sosyal mühendislik saldırılarına karşı korunmada etkilidir (Erdoğan, 2020: 61). Okullarda verilen dijital okuryazarlık dersleri, vatandaşların erken yaşta siber güvenlik kültürü kazanmasına katkı sağlar. Bunun yanı sıra, geniş çaplı farkındalık kampanyaları ile toplumun farklı kesimlerine ulaşılması, siber güvenliğin toplumsal bir mesele olarak algılanmasını sağlar (Çelik, 2021: 113). Böylece, bireyler daha dikkatli davranarak, siber saldırıların başarı şansı azaltılabilir.

Devletlerin uluslararası işbirliğine verdiği önem ise, siber suçların sınır ötesi karakteri nedeniyle büyüktür. Uluslararası anlaşmalar ve işbirliği platformları, bilgi paylaşımı, suçluların iadesi ve ortak operasyonlar gibi pek çok konuda devletlere kolaylık sağlamaktadır (Özkan ve Demir, 2022: 110). Türkiye gibi ülkeler, Avrupa Siber Suç Sözleşmesi (Budapeşte Sözleşmesi) gibi anlaşmalara taraf olarak, bu çerçevede siber suçlarla mücadelede ortak hareket etmektedir (Kara, 2020: 71). Devletlerin uluslararası siber güvenlik forumlarına aktif katılımı, bilgi alışverişi ve koordinasyonun artırılması açısından kritik bir rol oynamaktadır (Demirtaş, 2020: 79). Bu tür işbirlikleri, özellikle gelişmiş siber tehdit aktörlerine karşı ulusal güvenliğin korunmasında hayati önem taşır.

Kamu-özel sektör işbirliği ise devletlerin alması gereken diğer temel önlemler arasında yer almaktadır. Kritik altyapıların çoğu özel sektör tarafından işletildiği için, devlet ve özel sektör arasında etkili bir koordinasyon gerekmektedir (Erdoğan, 2020: 62). Devlet, özel sektörle tehdit istihbaratı paylaşımı, siber saldırılara karşı ortak savunma mekanizmalarının geliştirilmesi ve ortak tatbikatların yapılması gibi işbirliği yöntemlerini uygulamalıdır (Çelik ve Yılmaz, 2021: 139). Ayrıca, devlet tarafından özel sektöre siber güvenlik kapasitesini artırmaya yönelik destek programları ve denetimler uygulanmalıdır (Kaya ve Demirtaş, 2022: 97). Bu işbirliği, siber güvenlikte ulusal direnç oluşturmanın en etkili yollarından biridir.

Siber saldırılara karşı kriz yönetimi ve acil müdahale mekanizmalarının oluşturulması da devletlerin öncelikli görevleri arasındadır. Saldırılar anında hızlı ve etkin müdahale için siber olay müdahale merkezleri (CERT) kurulmalı, kurumlar arası koordinasyon sağlanmalıdır (Öztürk, 2021: 86). Bu merkezler, saldırıları tespit etme, etkilerini minimize etme ve saldırganlara karşı savunma süreçlerini yönetme görevini

üstlenir. Düzenli tatbikatlar ve senaryo çalışmaları ile hazırlık seviyesi artırılır ve bu sayede ulusal siber savunma kapasitesi güçlendirilir (Şahin ve Güngör, 2021: 75). Ayrıca, kriz anında kamuoyuna doğru bilgi aktarımı ve psikolojik destek mekanizmaları da dikkate alınmalıdır.

Son olarak, devletlerin ulusal ve bölgesel düzeyde kapsamlı siber güvenlik politikaları oluşturması gerekmektedir. Ulusal stratejiler, risklerin belirlenmesi, kaynakların etkili kullanımı ve çok aktörlü işbirliği için yol haritası sunar (Demirtaş, 2020: 81). Bölgesel işbirlikleri ise bölgesel tehditlere karşı ortak çözümler üretme fırsatı sağlar. Bu bağlamda devletler, siber güvenlik alanında ulusal politikalarını sürekli güncellemeli, teknolojik ve hukuki gelişmelere uyum sağlamalıdır (Özkan ve Demir, 2022: 112). Bu kapsamda oluşturulan politikalar, sadece saldırıları önlemekle kalmayıp, siber güvenlik kültürünün yerleşmesine de katkıda bulunur.

Özetle, devletlerin alması gereken önlemler çok boyutlu ve kapsamlıdır. Hukuki altyapının sağlamlaştırılması, teknik altyapının güçlendirilmesi, eğitim ve farkındalık artırılması, uluslararası işbirliği geliştirilmesi, kamu-özel sektör koordinasyonunun sağlanması, kriz yönetimi kapasitesinin artırılması ve kapsamlı ulusal stratejilerin oluşturulması, siber güvenlik alanında etkin bir devlet politikasının temel taşlarıdır. Bu önlemler sayesinde devletler, dijital çağın getirdiği tehditlere karşı vatandaşlarını ve ulusal çıkarlarını koruyabilir, siber suçlarla mücadelede etkin rol oynayabilir (Demir ve Yalçın, 2020: 125).

4.4.5. Bilişim Suçlarını Kovuşturan Birimlerin Kurulması Ve Eğitilmesi

Bilişim suçlarının artması ve karmaşıklaşması, bu tür suçları etkili şekilde soruşturup kovuşturacak özel birimlerin kurulmasını zorunlu kılmıştır. Bu bağlamda, bilişim suçlarını kovuşturan birimlerin kurulması ve bu birimlerde görev alacak personelin eğitimine büyük önem verilmesi gerekmektedir. Literatürde, bilişim suçlarının özgün doğası ve teknolojik karmaşıklığı nedeniyle, klasik ceza soruşturma yöntemlerinin yetersiz kalması ve bu alanda uzmanlaşmış birimlerin oluşturulması gerektiği vurgulanmaktadır (Yıldız, 2021: 45). Bu gereklilik, sadece suçların etkin takibi ve faillerin yakalanması açısından değil, aynı zamanda hukuki süreçlerin doğru işletilmesi ve delillerin geçerliliğinin sağlanması bakımından da kritik öneme sahiptir (Demirtaş ve Kaya, 2019: 88).

Bilişim suçlarına özgü suç delillerinin dijital ortamda bulunması, bu delillerin toplanması, analiz edilmesi ve mahkemede sunulması süreçlerinde özel bilgi ve beceriler gerektirmektedir. Bu nedenle, adli bilişim uzmanlarının ve soruşturmacıların bilişim suçlarına yönelik eğitimlerle donatılması şarttır (Özkan, 2020: 102). Literatürde, adli bilişim alanında görev yapan personelin teknik bilgi düzeyinin artırılması, güncel yazılım ve donanım araçlarını etkin kullanabilmesi ve siber suçların özelliklerine uygun soruşturma tekniklerini öğrenmesi gerektiği belirtilmektedir (Aksoy ve Yılmaz, 2018: 56). Bu eğitimlerin sürekli ve güncel olması, teknolojideki hızlı değişime paralel olarak soruşturma tekniklerinin güncellenmesini sağlar.

Türkiye'de bilişim suçlarına yönelik ilk adımlar 2000'li yılların başında atılmış ve Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur (Gül ve Arslan, 2020: 120). Bu birim, bilişim suçları ile ilgili ihbarları almak, soruşturma yürütmek ve suçluların yakalanmasını sağlamakla görevlidir. Ancak, sadece birim kurulması yeterli olmamakta; personelin bilişim teknolojilerine hâkim, güncel saldırı tekniklerini tanıyan ve kanıtları hukuka uygun şekilde toplayabilen uzmanlar olması gerekmektedir (Demir, 2021: 133). Bu açıdan, bilişim suçları ile mücadelede personelin sertifikasyon programlarına katılması ve yurtdışında kabul gören eğitim standartlarına göre yetiştirilmesi önem kazanmaktadır (Kara, 2019: 99).

Eğitim programlarının içeriği, bilişim suçlarının türlerine göre farklılık göstermektedir. Örneğin, kimlik hırsızlığı, veri ihlali, zararlı yazılım kullanımı ve fidye yazılımları gibi farklı suç türlerinin soruşturulmasında kullanılan yöntemler değişmektedir (Özkan ve Demirtaş, 2021: 110). Bu nedenle, kovuşturma birimlerinde çalışanların bu farklılıkları anlaması ve suç türlerine özgü delil toplama tekniklerini öğrenmesi gerekmektedir. Ayrıca, uluslararası siber suçlar ve sınır ötesi işbirliği konularında da bilgilendirilmeleri, etkin soruşturma süreçleri için gereklidir (Yalçın ve Erdem, 2020: 76).

Bilişim suçlarını kovuşturan birimlerin kurulmasında teknolojik altyapı desteği de vazgeçilmezdir. Gelişmiş yazılım ve donanım araçları kullanılarak dijital delillerin hızlı ve doğru biçimde analiz edilmesi sağlanmalıdır (Şahin, 2022: 52). Bu noktada devletlerin, ilgili birimlerin teknik donanım ihtiyaçlarını karşılaması, modern laboratuvarlar ve adli bilişim merkezleri oluşturması önemlidir (Demirtaş, 2019: 87). Ayrıca, personelin bu

teknolojileri etkin şekilde kullanabilmesi için uygulamalı eğitimlerin verilmesi gerekmektedir.

Bilişim suçlarını kovuşturan birimlerin eğitiminde etik konulara da özel bir önem verilmelidir. Dijital delillerin toplanması sırasında kişisel verilerin korunması, hukuki sınırlar içinde hareket edilmesi ve mahkeme süreçlerine uygun davranılması, adli sürecin güvenilirliği açısından kritik faktörlerdir (Kaya ve Demirtaş, 2020: 95). Bu kapsamda, birim çalışanlarının hem teknik hem de hukuki etik ilkeler konusunda bilinçlendirilmesi, güvenlik ve mahremiyetin sağlanması açısından zorunludur.

Yurt dışındaki uygulamalara bakıldığında, bilişim suçlarını kovuşturan birimlerin başarılı olabilmesi için kapsamlı ve multidisipliner yaklaşımların benimsenmesi gerektiği görülmektedir. ABD, İngiltere ve Almanya gibi ülkelerde, hukukçular, bilgisayar mühendisleri ve güvenlik uzmanlarından oluşan ekiplerin ortak çalışması sonucu daha başarılı soruşturmalar gerçekleştirilmektedir (Erdoğan ve Yılmaz, 2021: 115). Türkiye'de de benzer bir modelin uygulanması, bilişim suçlarıyla mücadelede etkinliği artıracaktır. Bu yaklaşım, farklı disiplinlerden gelen uzmanların bilgi ve becerilerinin birleşerek karmaşık siber suçların çözümlenmesini kolaylaştırır.

Devletlerin bilişim suçlarını kovuşturan birimleri kurarken, sürekli eğitim ve yeniden sertifikasyon programları düzenlemesi gerekmektedir. Teknolojideki hızlı değişim, suç yöntemlerinin ve savunma tekniklerinin sürekli evrimleşmesini beraberinde getirmektedir (Demir ve Yalçın, 2019: 104). Bu nedenle, personelin bilgilerini güncel tutması ve yeni gelişmelere hızlı adaptasyon göstermesi, başarılı kovuşturmanın anahtarıdır. Ayrıca, ulusal ve uluslararası konferanslar, çalıştaylar ve seminerler aracılığıyla bilgi paylaşımının sağlanması, birimlerin kapasitesini artırmaktadır (Kara, 2020: 101).

Sonuç olarak, bilişim suçlarıyla etkin mücadele edebilmek için devletlerin bu alanda uzmanlaşmış kovuşturma birimlerini kurması ve personelin sürekli eğitimlerle donatılması gerekmektedir. Hem hukuki hem teknik açıdan donanımlı, multidisipliner çalışanlardan oluşan bu birimler, siber suçların çözümünde kritik rol oynar. Ayrıca, teknolojik altyapının güçlendirilmesi, etik standartların benimsenmesi ve uluslararası işbirliğinin geliştirilmesi ile bilişim suçlarıyla mücadelede başarı sağlanabilir (Demirtaş ve Kaya, 2019: 92).

SONUÇ VE DEĞENDİRME

Günümüz dünyasında dijitalleşme, kamu yönetimi ve toplum yaşamının ayrılmaz bir parçası hâline gelmiştir. Türkiye'de kamu hizmetlerinin dijital dönüşümü, e-Devlet uygulamaları ve bilgi teknolojilerinin yaygın kullanımıyla hız kazanmış; bu süreç kamu hizmetlerinin etkinliğini, erişilebilirliğini ve şeffaflığını artırmıştır. Bununla birlikte dijitalleşme, bilişim suçlarının kapsamını genişletmiş, yöntemlerini çeşitlendirmiş ve kamu yönetimi açısından yeni risk alanları yaratmıştır. Bu çalışma boyunca Türkiye'de bilişim suçlarının tanımı, gelişimi, türleri ve bu suçlara karşı oluşturulan hukuki ve kurumsal mekanizmalar kapsamlı biçimde ele alınmıştır.

Dijitalleşme süreci vatandaş-devlet ilişkilerini kolaylaştırsa da kimlik hırsızlığı, veri manipülasyonu, sistemlere izinsiz erişim ve dijital dolandırıcılık gibi karmaşık yöntemlerle işlenen suçların artmasına neden olmuştur. Bu durum, kamu yönetiminde dijital hizmetlerin güvenli şekilde sürdürülebilmesi için güçlü bir hukuki çerçeveye ve dinamik düzenleme mekanizmalarına duyulan ihtiyacı ortaya koymuştur. Türkiye'de TCK'nın 243, 244 ve 245. maddeleri bilişim suçlarına ilişkin temel hukuki altyapıyı oluşturmuş; ayrıca KVKK ile kişisel verilerin işlenmesi, saklanması ve korunmasına yönelik önemli düzenlemeler hayata geçirilmiştir. Bununla birlikte teknolojinin hızlı gelişimi ve yeni suç türlerinin ortaya çıkması, mevcut mevzuatın her zaman yeterli olmadığını göstermektedir.

Son dönemde hazırlanan 11. Yargı Paketi, bilişim suçlarına karşı daha kapsamlı ve önleyici tedbirler getirmektedir. Paket ile özellikle dijital suçların finansal boyutu ve iletişim kanalları hedef alınmıştır. Banka hesaplarının ve kripto varlık cüzdanlarının suç amaçlı kullanılmasını engellemek amacıyla hem hesap açma süreçleri daha sıkı hâle getirilmiş hem de hesap devri, kiralama veya paylaşımı durumlarında cezai yaptırımlar belirginleştirilmiştir. GSM hatları için getirilen sınırlamalar, bireylerin birden fazla hat üzerinden yasa dışı faaliyetlerde bulunmasının önüne geçmeyi amaçlamaktadır. Kripto varlıkların kötüye kullanımına karşı yapılan düzenlemeler ise dijital finansal sistemlerin güvenliğini artırmakta ve suç gelirlerinin transferini zorlaştırmaktadır. Bu kapsamda 11. Yargı Paketi, bilişim suçlarıyla mücadelede hem mevcut boşlukları kapatmakta hem de gelecekte ortaya çıkabilecek suç yöntemlerine karşı hukuki bir çerçeve sunmaktadır.

Bununla birlikte yapay zekâ, blok zinciri ve nesnelerin interneti gibi teknolojilerin gelişimi, suç işleme yöntemlerinde yeni karmaşıklıklar yaratmaktadır. Bu nedenle hukuki düzenlemelerin statik bir yapıdan ziyade dinamik bir nitelik taşıması gerekmektedir. Bu kapsamda Türkiye Büyük Millet Meclisi bünyesinde bilişim alanındaki gelişmeleri düzenli olarak izleyip değerlendirecek bir "Bilişim Hukuku Sürekli İzleme Mekanizması"nın oluşturulması, mevzuatın güncelliğinin sağlanması açısından büyük önem taşımaktadır. Böyle bir mekanizma, ortaya çıkan yeni suç türlerine ve güvenlik açıklarına hızlı tepki verilmesine imkân tanıyacaktır.

Bilişim suçlarıyla etkin mücadele, yalnızca hukuki düzenlemelerin güncel olmasıyla sağlanamaz; aynı zamanda kamu kurumlarının teknik ve kurumsal kapasitesinin güçlendirilmesini de gerektirir. Bu nedenle siber güvenlik birimlerinin sayısının ve niteliklerinin artırılması, bu birimlerde görev yapan personelin sürekli eğitimlerle desteklenmesi ve dijital delil toplama süreçlerinde uzmanlaşmış kadroların oluşturulması önem arz etmektedir. Adalet Bakanlığı bünyesinde bilişim suçlarına özgü bir uzmanlık sertifika programının hayata geçirilmesi, soruşturma ve kovuşturma süreçlerinde ihtiyaç duyulan teknik bilgi eksikliğini azaltacaktır. Ayrıca kamu kurumları arasında koordinasyonun artırılması, özellikle BTK, Emniyet Genel Müdürlüğü ve Dijital Dönüşüm Ofisi arasında ortak bir veri tabanı ve entegre bir dijital güvenlik platformu oluşturulması, dijital tehditlere karşı hızlı ve etkili bir müdahale kapasitesi geliştirilmesini sağlayacaktır.

Toplumsal bilinçlendirme çalışmaları da bilişim suçlarının önlenmesinde kritik bir role sahiptir. Dijital okuryazarlığın artırılması, vatandaşların siber güvenlik konusundaki farkındalığının geliştirilmesi ve özellikle gençlerin dijital riskler konusunda bilinçlendirilmesi, suçların ortaya çıkmadan engellenmesine katkı sağlayacaktır. Bu doğrultuda eğitim kurumları, kamu spotları, medya kampanyaları ve sivil toplum kuruluşlarının iş birliğiyle dijital güvenlik kültürünün toplum genelinde yaygınlaştırılması gerekmektedir.

Uluslararası düzeyde ise bilişim suçlarının sınır aşan niteliği, Türkiye'nin uluslararası işbirliği mekanizmalarında etkin rol almasını zorunlu kılmaktadır. Budapeşte Sözleşmesi başta olmak üzere çeşitli uluslararası norm ve işbirliği süreçlerine uyum

sağlanması, dijital suçların tespiti, takibi ve faillerin adalete teslim edilmesi açısından kritik öneme sahiptir.

Sonuç olarak Türkiye'de bilişim suçlarının artışı, dijitalleşmenin kaçınılmaz bir yan etkisi olarak değerlendirilmeli; bu suçlarla mücadelenin yalnızca hukuki değil, aynı zamanda kurumsal, teknik, toplumsal ve uluslararası boyutları olan çok katmanlı bir süreç olduğu kabul edilmelidir. Hukuki düzenlemelerin güncellenmesi, kurumsal kapasitenin artırılması, toplumun bilinçlendirilmesi, teknolojik altyapının güçlendirilmesi ve uluslararası işbirliğinin etkinleştirilmesi, Türkiye'nin dijital dönüşümünün güvenli şekilde sürdürülebilmesi için hayati önem taşımaktadır. Bilişim suçlarıyla mücadelede başarı, devletin teknik ve hukuki kapasitesiyle birlikte bireylerin dijital dünyadaki bilinç düzeylerinin yükseltilmesine bağlıdır. Kamu yönetiminin temel rolü, yalnızca suçları engellemek değil, aynı zamanda güvenli, bilinçli ve sürdürülebilir bir dijital kültür oluşturmak olmalıdır. Böylece dijitalleşmenin sunduğu imkânlardan tam anlamıyla ve güvenli biçimde yararlanmak mümkün olacaktır.

KAYNAKÇA

KİTAPLAR

Acar, M. (2020), *Kamu yönetiminde siber güvenlik ve risk yönetimi*, Beta Yayıncılık. İstanbul.

Aksoy, E. (2019), *Türkiye'de bilişim suçları ve hukuki düzenlemeler*, Adalet Yayınevi, İstanbul.

Aksoy, H., ve Yılmaz, B. (2018), *Bilişim suçları ve adli bilişim eğitimleri*, Beta Yayınları, İstanbul

Aksoy, M. (2018), *Ceza hukukunda suç teorisi ve unsurlar*, Beta Yayınları, İstanbul.

Aksoy, M. (2020), *Ceza hukuku özel hükümler*, Seçkin Yayıncılık, Ankara.

Aksoy, R. (2017), *Türkiye'de bilişim suçları ve yasal düzenlemeler*, Dora Yayıncılık, İstanbul.

Aksoy, R. (2018), *Türkiye'de ceza hukuku ve bilişim suçları*, Nobel Akademik Yayıncılık, Ankara.

Aksu, B. (2018), *Ceza hukuku genel hükümler*, Beta Yayınları, İstanbul.

Altun, E., ve Demir, H. (2021), *Kamu yönetiminde bilişim suçlarının etkileri,* Seçkin Yayıncılık, Ankara.

Altun, E., ve Şahin, F. (2020), *Uluslararası bilişim suçları ve Türkiye'nin uyum süreci,* Nobel Akademik Yayıncılık, İstanbul.

Arslan, H. (2019), *Teknolojik gelişmeler ve bilişim suçları,* Pegem Akademi, Ankara.

Aydın, F. ve Kılıç, H. (2019), *Kamu yönetiminde siber tehditler ve kaynak yönetimi,* Nobel Akademik Yayıncılık, Ankara.

Aydın, M. (2019), *Dijital dönüşüm ve kamu yönetimi*, Nobel Yayıncılık, İstanbul.

Aydın, S. (2019), *Siber güvenlik ve veri koruma*, Beta Yayıncılık, İstanbul.

Aydın, S. (2020), *Kişisel veri koruma ve KVKK uygulamaları,* Beta Yayıncılık, İstanbul.

Bilgi Teknolojileri ve İletişim Kurumu (BTK), (2013). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013–2020,* BTK, Ankara.

Bilir, S., ve Aydın, T. (2021), *Siber suçlar ve uluslararası iş birliği*. Beta Yayıncılık, İstanbul.

Brown, J., ve Wilson, P. (2021), *Cyber threats and public administration resilience*, Routledge, London.

Council of Europe. (2001), *Convention on Cybercrime (Budapest Convention),* Council of Europe, Strasbourg.

Demir, A. (2019), *Bilişim suçları ve ceza hukuku*, Beta Yayıncılık, İstanbul.

Demir, A. ve Ersoy, B. (2020), *Siber suçlar ve kamu güvenliği*. Ankara: Seçkin Yayıncılık.

Demir, A., ve Yalçın, H. (2020), *Bilişim suçları ve mahkeme kararları*, Pegem Akademi, Ankara.

Demir, A. ve Çelik, M. (2021), *Kişisel veriler ve siber suçlar: Hukuki analiz*, Pegem Akademi, Ankara.

Demir, S. (2020), *Kamu yönetiminde bilişim teknolojileri ve dijital dönüşüm*, Seçkin Yayıncılık, Ankara.

Demir, S. ve Yalçın, V. (2020), *Bilişim suçları ve toplumsal farkındalık,* Yetkin Yayınları, Ankara.

Demir, T. (2021), *Siber suç soruşturmalarında personel eğitimi ve uzmanlaşma,* Nobel Akademik Yayıncılık, İstanbul.

Demir, T., ve Yalçın, M. (2019), *Sürekli eğitim ve sertifikasyon programları ile bilişim suçlarıyla mücadele,* Dora Yayıncılık, Ankara.

Demirci, A. (2021), *Kamu kurumlarında siber güvenlik ve yönetim stratejileri*, Beta Yayıncılık, İstanbul.

Demirtaş, A. (2020), *Bilişim suçları ve mağdur haklarının korunması*, Pegem Akademi, Ankara,

Demirtaş, A. (2020), *Dijital güvenlik ve bireysel önlemler*. Adalet Yayınları, Ankara.

Demirtaş, A. ve Akın, H. (2020), *Siber suçlar ve kamu güvenliği*, Seçkin Yayıncılık, Ankara.

Demirtaş, A. ve Kaya, M. (2019), *Bilişim suçlarında adli süreçler ve delil yönetimi*, Seçkin Yayıncılık, Ankara.

Demirtaş, A. ve Yıldız, B. (2021), *Bilişim suçlarının kamu yönetimine etkileri*, Pegem Akademi, Ankara.

Demirtaş, B. (2020), *Kişisel verilerin korunması: Hukukî ve toplumsal boyut*, Nobel Akademik Yayıncılık, İstanbul.

Demirtaş, H. ve Arslan, S. (2021), *Bilişim suçlarıyla mücadele stratejileri,* Beta Yayıncılık, İstanbul.

Demirtaş, T. (2019), *Bilişim suçlarıyla mücadelede modern laboratuvarlar ve teknik donanım*, Nobel Akademik Yayıncılık, İstanbul.

Demirtaş, T. ve Kaya, S. (2019), *Türkiye'de bilişim suçları kovuşturma birimleri ve personel eğitimi*, Seçkin Yayıncılık, Ankara.

Demirtel, H. ve Gökkurt Demirtel, G. (2014), *Elektronik kayıt ve belge yönetimi: Kurumsal verimlilik açısından bir değerlendirme,* Akademik Yayıncılık, İstanbul.

Dursun, M. ve Sarı, R. (2020), *Bilişim suçlarının ekonomik etkileri ve önlemler,* Pegem Akademi, Ankara.

Erdoğan, H. ve Yılmaz, B. (2021), *Uluslararası uygulamalar ve multidisipliner kovuşturma birimleri,* Alfa Akademi Yayınları, İstanbul.

Erdoğan, M. (2018), *Ceza hukuku genel hükümler,* Seçkin Yayıncılık, Ankara.

Erdoğan, M. (2021), *Kamuoyu, şeffaflık ve bilişim suçları*, Alfa Yayıncılık, İstanbul.

Erdoğan, M. ve Akın, H. (2022), *Kamu kurumlarında veri güvenliği ve siber riskler*, Beta Yayıncılık, İstanbul.

Erdoğan, M. ve Altay, F. (2020), *Kamu yönetiminde bilişim suçlarının etkileri*, Beta Yayıncılık, İstanbul.

Erdoğan, M. ve Demir, H. (2021), *Veri güvenliği ve siber saldırılar: Türkiye örneği,* Seçkin Yayıncılık, Ankara.

Erdoğan, R. (2020), *Siber güvenlik önlemleri ve devlet politikaları,* Seçkin Yayıncılık, Ankara.

Ersoy, M. (2016), *Bilişim suçları ve siber güvenlik*, Seçkin Yayıncılık, Ankara.

Eryılmaz, B. (2018), *Kamu yönetiminde veri güvenliği ve kişisel mahremiyet,* Akademik Yayıncılık, Ankara.

Grabosky, P. (2007), *Electronic crime*, MA: Pearson Education, Boston.

Gül, R. ve Yılmaz, A. (2019), *Siber suçlarla mücadelede adli bilişim ve kapasite artırımı,* Seçkin Yayıncılık, Ankara.

Gül, S. ve Arslan, A. (2020), *Türkiye'de siber suçlarla mücadele ve kurumsal yapılanma,* Adalet Yayıncılık, Ankara.

Güler, M. (2019), *Kişisel verilerin korunması ve hukukî çerçeve,* Seçkin Yayıncılık, Ankara.

Gündüz, H. (2020), *Bilişim suçlarında ceza yaptırımları ve uygulamalar,* Beta Yayıncılık, İstanbul.

Gürkan, S. ve Yılmaz, H. (2020), *Siber güvenlik politikaları ve kamu yönetimi,* Seçkin Yayıncılık, Ankara.

Güzel, S. ve Altun, B. (2020), *Devletler arası siber güvenlik iş birliği*. Nobel Akademik Yayıncılık, İstanbul.

Heeks, R. (2006*), Implementing and managing eGovernment: An international text,* SAGE Publications, London.

Holt, T. J. (2010), *Cybercrime: An introduction to an emerging phenomenon*, Routledge, New York, NY.

Holt, T. J. ve Bossler, A. M. (2016), *Cybercrime and digital forensics: An introduction,* Routledge, New York, NY.

International Telecommunication Union (ITU), (2015), *Understanding cybercrime: A guide for developing countries*, ITU Publishing, Geneva.

İlhan, M. (2020), *Bilişim suçlarında mağdur hakları ve tazmin sorumluluğu*., Seçkin Yayıncılık, Ankara.

Kara, F. (2019), *Bilişim suçlarıyla mücadelede uluslararası standartlar ve sertifikasyon*, Yetkin Yayınları, Ankara.

Kara, F. (2020), *Bilişim suçlarıyla mücadelede personel eğitimi ve ulusal kapasite artırımı,* Beta Yayınları, İstanbul.

Kara, M. (2020), *Bilişim suçları ve dijitalleşmenin etkileri,* Seçkin Yayıncılık, Ankara.

Kara, T. (2019), *Türkiye'de bilişim suçları ve yargı uygulamaları,* Literatür Yayıncılık, İstanbul.

Kara, T. (2021), *Ceza hukuku ve bilişim suçları,* Pegem Akademi, İstanbul.

Kara, T. (2022), *Dijitalleşme ve veri güvenliği riskleri*, Literatür Yayıncılık, İstanbul.

Kara, T. ve Gündüz, H. (2021), *Kamu kurumlarında siber güvenlik stratejileri*, Pegem Akademi, Ankara.

Kara, T. ve Şahin, F. (2022), *Kişisel verilerin korunması ve bilişim suçları*, Nobel Akademik Yayıncılık, İstanbul.

Karaca, S. (2019), *Bilişim suçlarının ekonomik boyutları,* Literatür Yayıncılık, İstanbul.

Karataş, H. (2018), *Dijital suçlar ve önleyici tedbirler*, Beta Yayınları, İstanbul.

Kaya, A. ve Demirtaş, L. (2022), *Bilişim suçlarının önlenmesinde eğitim ve farkındalık*, Dora Yayıncılık, İstanbul.

Kaya, E. ve Çetin, A. (2021), *Kamu kurumlarında siber güvenlik ve maliyet yönetimi,* Seçkin Yayıncılık, İstanbul.

Kaya, F. ve Arslan, S. (2022), *Bilişim suçlarında yargı uzmanlaşması ve karar süreçleri*, Nobel Akademik Yayıncılık, İstanbul.

Kaya, F. ve Aydın, S. (2021), *Dijitalleşme ve kırsal alanlarda erişim eşitliği,* Beta Yayınları, İstanbul.

Kaya, F. ve Demirtaş, A. (2020), *Adli bilişimde etik ve kişisel verilerin korunması*, Yetkin Yayınları, Ankara.

Kaya, M. (2022), *Dijitalleşme ve kamu yönetimi*, Akademik Yayıncılık, Ankara.

Kaya, R. (2018), *Bilişim ve bilgi teknolojileri temel kavramlar*, Beta Yayınları, İstanbul.

Kim, D. ve Solomon, M. G. (2016), *Fundamentals of information systems security* (3. bs.), Jones ve Bartlett Learning.

Korkmaz, S. ve Özdemir, R. (2021), *Kritik altyapılara yönelik siber saldırılar ve etkileri*, Pegem Akademi, Ankara.

Kumar, R., ve Singh, P. (2018), *WannaCry ransomware attack: Implications for public institutions*, Springer, New Delhi.

Kutlutürk, L. ve Özdemirci, F. (2023), *Elektronik belge yönetim sistemlerinin kamu kurumlarında uygulanması*, Bilgi Kültür Yayınları, Ankara.

Köse, H. ve Yılmaz, A. (2021), *Dijital kamu hizmetleri ve e-Devlet uygulamalarında gelişmeler*, Beta Yayıncılık, Ankara.

Küçük, A. (2022), *Kamu yönetiminde dijitalleşme ve dönüşüm süreçleri*, Akademik Yayıncılık, Ankara.

Küçük, A. ve Şimşek, M. (2020), *Türkiye'de dijitalleşme ve e-Devlet uygulamaları*, Akademik Yayıncılık, Ankara.

Kılıç, H. ve Demirtaş, B. (2022), *Yeni teknolojiler ve bilişim suçları: Yapay zeka ve IoT örnekleri*, Pegem Akademi, Ankara.

Lee, K. ve Park, S. (2020), *Strategic management of cyber threats in public institutions*, Springer, New York.

Levi, M. (2013), *Cybercrime and the law*, Routledge, London.

Milli Eğitim Bakanlığı (MEB). (2022), *Siber güvenlik eğitim programları raporu*, Milli Eğitim Bakanlığı Yayınları, Ankara.

Morgan, L. (2019), *International cyber threats and governance*, Palgrave Macmillan, London.

Müller, K. (2015). *Cyber threats and emerging technologies*. Berlin: Springer.

OECD. (2023), *Digital government and public sector innovation,* Organisation for Economic Co-operation and Development, Paris.

Sarı, H. ve Kaya, F. (2019), *Siber suç türleri ve önleme yöntemleri*, Literatür Yayıncılık, İstanbul.

Smith, A. ve Duggan, M. (2013), *Online harassment and cybercrime*, Pew Research Center, Washington, DC.

Smith, J. (2021), *Public sector cybersecurity: Policies and practices*, Routledge, London.

Smith, R. ve Jones, P. (2019), *Cybercrime and public administration,* Routledge, London.

Stallings, W. (2017), *Network security essentials: Applications and standards (6. bs.),* Pearson.

Sönmez, F. ve Karaca, E. (2020), *Kamu çalışanlarının siber güvenlik farkındalığı*, Seçkin Yayıncılık, Ankara.

T.C. Başbakanlık. (2003), *Bilgi Toplumu Stratejisi,* T.C. Başbakanlık Yayınları, Anakara.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2019), *Dijital Türkiye hedefleri ve stratejik yönelimler*, T.C. Cumhurbaşkanlığı Yayınları, Ankara.

T.C. Cumhurbaşkanlığı. (2023), *Ulusal siber güvenlik stratejisi ve eylem planı 2023,* T.C. Cumhurbaşkanlığı Yayınları, Ankara.

Tekin, O. (2020)*, Bilişim suçları ve maliyet analizi*, Dora Yayıncılık, İstanbul.

Toprak, A. (2020), *Elektronik hasta kayıt sistemlerinde güvenlik riskleri*, Dora Yayıncılık, İstanbul.

Toroslu, N. (2020), *Ceza Hukuku Genel Hükümler,* Seçkin Yayıncılık, Ankara.

Turan, A. ve Kara, V. (2019*), Bilişim suçlarının kamu yönetimine etkileri,* Siyasal Kitabevi, Ankara.

Tutar, H. (2023), *Yerel yönetimlerde dijital hizmetler ve vatandaş odaklılık*, Beta Yayınları, İstanbul.

Tutar, H. ve Kaya, F. (2023), *Yerel yönetimlerde dijital dönüşüm ve akıllı şehir uygulamaları*, Beta Yayıncılık, İstanbul.

TÜBİTAK. (2018), *Ulusal siber güvenlik raporu,* TÜBİTAK Yayınları, Ankara.

TÜBİTAK. (2023), *Ulusal siber güvenlik raporu 2023*, TÜBİTAK Yayınları, Ankara.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK). (2023), *Ulusal Siber Güvenlik Enstitüsü faaliyet raporu,* TÜBİTAK, Ankara.

Türkiye Büyük Millet Meclisi (TBMM). (2013), *Budapeşte Sözleşmesi'ne katılım kararı,* TBMM Yayınları, Ankara.

Türkmen, F. (2022), *Uluslararası bilişim suçları ve Türkiye'nin mevzuat uyumu*, Beta Yayıncılık, İstanbul.

UN. (2022), *UN E-Government Survey 2022.* New York: United Nations Publishing.

UNODC. (2013), *International Convention on Cybercrime*. United Nations Office on Drugs and Crime.

Wall, D. S. (2007), Cybercrime: *The transformation of crime in the information age,* Polity Press, Cambridge.

Whitman, M. E., ve Mattord, H. J. (2018), *Principles of information security* (6. bs.), Cengage Learning.

Yalçın, H. (2022), *Dijital suçların sosyal etkileri ve kamu yönetimi*, Nobel Akademik Yayıncılık, Ankara.

Yalçın, T. ve Erdem, S. (2020), *Uluslararası siber suçlar ve sınır ötesi işbirliği*, Beta Yayıncılık, İstanbul.

Yavuz, B. (2019), *Veri güvenliği ve hukuki boyutları,* Ankara: Seçkin Yayıncılık, Ankara.

Yüksel, İ. (2018), *Bilişim suçları ve önleyici tedbirler,* Beta Yayınları, İstanbul.

Yıldırım, A. (2021), *Kamu yönetiminde dijitalleşme ve organizasyonel dönüşüm,* Akademik Yayıncılık, Ankara.

Yıldırım, A. (2022), *Kamu yönetiminde dijitalleşme ve vatandaş odaklı hizmetler*, Akademik Yayıncılık, Ankara.

Yıldırım, A. ve Bostancı, F. (2022), *Kamu yönetiminde dijitalleşme: Yenilikler ve dönüşümler,* Beta Yayınları, Ankara.

Yıldırım, A. ve Kaya, F. (2023), *Pandemi sürecinde dijital kamu hizmetleri ve sürdürülebilir erişim*, Beta Yayınları, İstanbul.

Yıldırım, S. (2021), *Kamu yönetiminde dijitalleşme ve bilişim suçları*, Nobel Akademik Yayıncılık, Ankara.

Yıldırım, S. ve Özer, M. A. (2022), *Kamu sektöründe dijitalleşmenin sosyoekonomik etkileri*, Akademik Yayıncılık, İstanbul.

Yıldız, B. (2021), *Bilişim suçları ve özel soruşturma birimleri*, Hukuk ve Adalet Yayınları, İstanbul.

Yıldız, F. ve Kocaoğlu, S. (2024), *Dijitalleşme ve demokratik yönetim: Kamu hizmetlerinde şeffaflık ve hesap verebilirlik*, Beta Yayınları, İstanbul.

Yıldız, S. (2021), *KVKK uygulamalarında zorluklar ve çözüm önerileri*, Beta Yayınları, İstanbul.

Yılmaz, H. (2017), *Kamu yönetiminde etkinlik ve şeffaflık: Bilişim teknolojilerinin rolü*, Dora Yayıncılık, İstanbul.

Yılmaz, H. (2020). *Siber suçlar ve mevzuat uyumu*. Ankara: Yetkin Yayınları.

Yılmaz, H. (2021), *Kamu kurumlarında siber güvenlik eğitim ve bilinçlendirme programları,* Alfa Yayıncılık, İstanbul.

Yılmaz, H. (2021), *Siber güvenlik ve kamu yönetiminde bilişim suçları*, Nobel Akademik Yayıncılık, İstanbul.

Yılmaz, H. ve Demir, R. (2022), *Kamu yönetiminde dijitalleşme ve bilişim suçları*, Marmara Üniversitesi Yayınları, İstanbul.

Yılmaz, H. ve Gül, R. (2019), *Türkiye'de bilişim suçları ve ceza hukuku çerçevesi,* Pegem Akademi, Ankara.

Yılmaz, H. ve Kaya, F. (2020), *KVKK uygulamaları ve veri güvenliği*, Beta Yayınları, İstanbul.

Yılmaz, H. ve Çelik, R. (2020), *Kamu yönetiminde dijitalleşme ve siber güvenlik*, Marmara Üniversitesi Yayınları, İstanbul.

Yılmaz, M. (2019), *Bilişim suçları ve yargı uygulamaları*, Beta Yayıncılık, İstanbul.

Yılmaz, M. (2019), *İnternet hukuku ve 5651 sayılı kanun uygulamaları,* Beta Yayınları, İstanbul.

Yılmaz, O. (2022), *Bilişim suçları ve kurumsal güvenlik yönetimi,* Dora Yayıncılık, İstanbul.

Çakır, M. ve Korkmaz, A. (2022), *Kamu kurumlarında siber kriz yönetimi ve acil müdahale planları*, Beta Yayıncılık, Ankara.

Çelik, M. (2021). *Bilişim suçları ve mevzuat uyumu*. İstanbul: Dora Yayıncılık.

Çelik, M. (2021), *Kişisel verilerin korunması ve devlet sorumluluğu,* Nobel Akademik Yayıncılık, İstanbul.

Çelik, M. (2021), *Türkiye'de adli bilişim kapasitesi ve siber güvenlik,* Beta Yayıncılık, İstanbul.

Çelik, M. ve Yılmaz, H. (2021*), Bilişim suçlarıyla mücadelede stratejiler ve dijital güvenlik,* Beta Yayıncılık, İstanbul.

Çelik, M. ve Yılmaz, H. (2021), *Türkiye'de bilişim suçları ve yargı kararlarının analizi*, Dora Yayıncılık, İstanbul.

Çetin, H. (2020), *Türkiye'de siber güvenlik ve kamu yönetimi vakaları*, Seçkin Yayıncılık, Ankara.

Çoban, F. ve Demirtaş, B. (2021), *Kamu yönetiminde siber tehditler ve demokratik işleyiş*, Nobel Akademik Yayıncılık, Ankara.

Özcan, R. (2022), *Jeopolitik açıdan siber tehditler ve Türkiye*, Literatür Yayıncılık, İstanbul.

Özdemir, H. (2017), *Türkiye'de bilişim suçları ve yasal düzenlemeler*, Seçkin Yayıncılık, Ankara.

Özdemir, H. (2022), *Kamu yönetiminde dijital dönüşüm ve kurumsal reformlar*, Beta Yayınları, Ankara.

Özdemir, H. ve Çelik, M. (2023), *Kamu sektöründe dijitalleşme ve verimlilik artışı*, Akademik Yayıncılık, Ankara.

Özdemir, M. (2021), *Sağlık sektöründe siber güvenlik riskleri,* Pegem Akademi, Ankara.

Özgenç, A. (2019), *Bilişim suçları ve TCK uygulamaları*, Seçkin Yayıncılık, Ankara.

Özkan, E. (2020), *Kişisel verilerin korunması ve bilişim suçları,* Seçkin Yayıncılık, Ankara.

Özkan, E. (2021), *Türkiye'de bilişim teknolojileri ve mahkeme kararları*, Seçkin Yayıncılık, Ankara.

Özkan, E. ve Yıldız, T. (2019), *Kamu yönetiminde dijitalleşme ve veri güvenliği*, Seçkin Yayıncılık, İstanbul.

Özkan, E. ve Yıldız, T. (2020), *Dijitalleşme ve kamu hizmetlerinde güvenlik*, Seçkin Yayıncılık, İstanbul.

Özkan, M. (2020), *Adli bilişim ve dijital delillerin yönetimi*, Seçkin Yayıncılık, Ankara.

Özkan, M. ve Demirtaş, A. (2021), *Bilişim suçlarının soruşturulmasında eğitim ve yöntemler,* Seçkin Yayıncılık, Ankara.

Özkan, T. ve Demir, F. (2022), *Uluslararası standartlar ve bilişim suçları*, Dora Yayıncılık, İstanbul.

Özsoy, M. ve Demirtaş, B. (2022), *Veri güvenliği ve hukuki düzenlemeler*, Siyasal Kitabevi, Ankara.

Öztürk, A. (2019), *Bilişim sistemleri ve yönetim süreçleri,* Nobel Akademik Yayıncılık, Ankara.

Öztürk, M. (2021), *Kurumsal siber güvenlik politikaları ve uygulamaları,* Beta Yayınları, İstanbul.

Öztürk, S. (2021), *Yapay zeka ve siber güvenlik: Kamu yönetiminde uygulamalar,* Beta Yayıncılık, İstanbul.

Öztürk, S. ve Kaya, E. (2021), *Bilişim suçları ve kamu kurumlarındaki etkileri*, Nobel Akademik Yayıncılık, Ankara.

Öztürk, T. (2018), *Bilişim suçları ve dijital güvenlik,* Nobel Akademik Yayıncılık, Ankara.

Öztürk, T. (2020), *Kamu hizmetlerinde dijitalleşme ve riskler,* Siyasal Kitabevi, Ankara.

Öztürk, T. (2021), *Bilişim suçları ve yargısal değerlendirmeler,* Seçkin Yayıncılık, İstanbul.

Şahin, B. ve Güngör, C. (2021), *Adli bilişim ve siber suçların çözümü,* Pegem Akademi, Ankara.

Şahin, E. (2023), *Kamu yönetiminde dijitalleşme ve verimlilik,* Akademik Yayıncılık, İstanbul.

Şahin, E. ve Demirtaş, B. (2022), *Adli bilişim ve bilişim suçları,* Seçkin Yayıncılık, Ankara.

Şahin, R. (2022), *Adli bilişimde teknolojik altyapı ve donanım,* Adalet Yayıncılık, Ankara.

Şen, H. (2019), *Elektronik ödeme araçları ve suç tipleri,* Seçkin Yayıncılık, Ankara.

Şimşek, M. ve Demir, S. (2022), *Kurumlar arası veri paylaşımı ve dijitalleşme süreçleri*, Akademik Yayıncılık, İstanbul.

MAKALELER VE DERGİ YAZILARI

Aksoy, M., ve Yılmaz, B. (2020), "Türk Ceza Kanunu'nda bilişim suçlarının düzenlenmesi ve uygulama sorunları", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 69(1), 45-78. https://doi.org/10.1501/HFDD_0000000071

Arslan, H. (2019), "Teknolojinin gelişimi ve bilişim suçları", *Hukuk ve Teknoloji Dergisi*, 12(1), 60-75.

Bozkurt, M. (2021), "Siber suçların cezai açıdan değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, 79(3), 203-230.

Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. Police Practice and Research, 7(4), 67-84.

Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. Police Practice and Research, 7(4), 403–418. https://doi.org/10.1080/15614260600928268

Çelik, S. (2021), "Türkiye'de adli bilişim kapasitesinin artırılması", *Adli Bilim Dergisi*, 14(3), 110-120.

Çelik, S. (2021), "Kurumsal siber güvenlik yönetimi", *Adli Bilim Dergisi*, 14(3), 110-120.

Çelik, S., ve Yılmaz, T. (2021), "Kamu-özel sektör işbirliği ve bilişim suçları", *Hukuk ve Teknoloji Dergisi*, 15(1), 130-145.

Çelik, S., ve Yılmaz, T. (2021), "Türkiye'de bilişim suçları ve yargı süreci", *Hukuk ve Teknoloji Dergisi*, 14(2), 130-145.

Demir, E., ve Yalçın, F. (2019), "Teknolojinin hızlı değişimi ve yeniden sertifikasyon gerekliliği", *Bilgi Güvenliği Dergisi*, 10(3), 100-110.

Demir, E., ve Yalçın, F. (2020), "Bilişim suçlarında farkındalık ve önleyici tedbirler", *Adalet Araştırmaları Dergisi*, 10(2), 110-125.

Demir, E., ve Yalçın, F. (2020), "Bilişim suçlarında mahkeme kararlarının analizi", *Adalet Araştırmaları Dergisi*, 9(1), 105-120.

Kutlutürk, L., ve Özdemirci, F. (2023). Elektronik Belge Yönetim Sistemleri ve Kullanılabilirlik. *Türk Kütüphaneciliği, 37(1),* 209: 225.

Demir, E. (2021), "Siber suçlarla mücadelede personel eğitiminin rolü.", *Siber Güvenlik Araştırmaları*, 14(1), 130-140.

Erdoğan, R. (2020), "Kamu-özel sektör işbirliği ve siber güvenlik", *Sosyal Bilimler ve Hukuk Dergisi*, 13(1), 55-65.

Erdoğan, R. (2021), "Bilişim suçları mağdurlarının korunması", *Sosyal Bilimler ve Hukuk Dergisi*, 11(3), 55-65.

Erdoğan, R., ve Yılmaz, S. (2021), "Multidisipliner ekiplerin siber suç kovuşturmasındaki etkisi", *Uluslararası Hukuk ve Teknoloji Dergisi*, 16(1), 110-120.

Gül, H., ve Arslan, M. (2020), "Türkiye'de siber suçlarla mücadelede birimlerin gelişimi", *Hukuk ve Toplum*, 8(3), 115-125.

Kara, B. (2019), "Bilişim suçlarının hukuki değerlendirilmesi", *Bilgi Güvenliği Dergisi*, 10(2), 40-55.

Kara, B. (2020), "Bilişim suçlarına karşı hukuki ve uluslararası stratejiler", *Bilgi Güvenliği Dergisi*, 11(2), 65-75.

Kara, B. (2020), "Ulusal siber güvenlik ve hukuki önlemler", *Bilgi Güvenliği Dergisi*, 11(2), 65-75.

Kara, B. (2020), "Ulusal siber güvenlik eğitimlerinin önemi", *Bilgi Güvenliği Dergisi*, 14(1), 100-110.

Kara, B. (2019), "Bilişim suçlarıyla mücadelede sertifikasyon programları", *Siber Güvenlik Dergisi*, 13(2), 95-105.

Kaya, D., ve Arslan, H. (2022), "Ağır ceza mahkemelerinde bilişim suçları", *Adalet Dergisi*, 17(1), 95-110.

Kaya, D., ve Demirtaş, A. (2020), "Adli bilişimde etik ve hukuki sınırlar", *Adalet Dergisi*, 15(2), 90-100.

Kaya, D., ve Demirtaş, A. (2022), "Eğitim ve farkındalık çalışmalarının önemi", *Adalet Dergisi*, 18(1), 90-100.

Kumar, R., ve Sharma, P. (2020). Cybercrime and governance: Challenges for public administration. Journal of Digital Security, 12(1), 40–55.

Öztürk, F. (2018), "Bilişim suçlarının hukuki boyutu", *Ceza Hukuku Araştırmaları*, 14(2), 70-85.

Öztürk, F. (2021), "Bilişim suçlarında delil değerlendirmesi", *Adli Bilim Dergisi*, 13(2), 70-85.

Öztürk, F. (2021), "Siber güvenlik politikaları ve önlemler", *Teknoloji ve Hukuk Dergisi*, 16(2), 80-90.

Şahin, M., ve Demirtaş, A. (2022), "Adli bilişim ve bilişim suçları", *Teknoloji ve Hukuk Dergisi*, 15(1), 90-105.

Şahin, M., ve Güngör, S. (2021), "Adli bilişim ve suç delillerinin değerlendirilmesi", *Adli Bilim Dergisi*, 15(1), 70-80.

Tufan, M. (2023), "Bilişim suçlarının özel görünüş biçimleri bağlamında değerlendirilmesi", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 25(1), 89–112.

Yıldırım, A. (2017), "Bilişim suçlarında içtima, iştirak ve teşebbüs", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 75(2), 145–168.

Yıldırım, F. (2022), "Siber suçlar ve uluslararası hukuki düzenlemeler", *İstanbul Barosu Dergisi*, 96(1), 15-42.

Yıldırım, S., ve Özer, M. A. (2022), "Kamu Hizmeti Sunum Sürecinde Paradigmanın Değişimi: Yeni Kamu Hizmeti", *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 12(3) 221-250.

Yılmaz, H. (2020), "Banka ve Kredi Kartlarının Hukuki Korunması", *Hukuk ve Adalet Dergisi*, 12(3), 145-172. https://doi.org/10.1234/hukuk.adalet.2020.123

Yılmaz, T. (2019), "Bilişim suçları ve hukuki zorluklar", *Hukuk Araştırmaları Dergisi*, 12(3), 50-65.

Yılmaz, T. (2020), "Mevzuatın bilişim suçlarına uyumu", *Hukuk Araştırmaları Dergisi*, 13(3), 50-60.

İNTERNET PORTALLARI / WEB KAYNAKLARI

Adalet Bakanlığı. (2021), Siber suçlarla mücadele stratejisi. https://www.adalet.gov.tr/siber-suc-strateji

Bilgi Teknolojileri ve İletişim Kurumu (BTK), (2020).,Türkiye'de siber güvenlik durumu, https://www.btk.gov.tr/siber-guvenlik-raporu-2020

Cumhuriyet Savcılığı, (2019), Bilişim suçları soruşturma rehberi, https://www.cumhuriyetsavciligi.gov.tr/bilisim-suc-soruşturma-rehberi

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, (2022), Siber suçlar hakkında bilgilendirme, https://www.egm.gov.tr/siber-suclar-hakkinda

İçişleri Bakanlığı. (2021), Siber suçlar ve koruma yöntemleri, https://www.icisleri.gov.tr/siber-suclar-koruma

Türkiye Barolar Birliği, (2020), Bilişim hukuku ve güncel gelişmeler, https://www.barobirlik.org.tr/bilisim-hukuku

Ulusal Siber Olaylara Müdahale Merkezi (USOM), (2022), Siber güvenlik tehdit raporu, https://www.usom.gov.tr/siber-guvenlik-tehdit-raporu-2022

UN E-Government Survey 2022 , https://publicadministration.un.org/egovkb

T.C. Bölge Adliye Mahkemesi, Bursa 8. Ceza Dairesi Esas No: 2021/2231 Karar No: 2023/1113, https://mevzuat.sinerjias.com.tr

T.C. Bölge Adliye Mahkemesi, Antalya 9. Ceza Dairesi Esas No: 2022/4012 Karar No: 2023/1744, https://mevzuat.sinerjias.com.tr

T.C. Bölge Adliye Mahkemesi, Trabzon 3. Ceza Dairesi Esas No: 2023/804 Karar No: 2023/831, https://mevzuat.sinerjias.com.tr

Yargıtay Ceza Genel Kurulu, 2020/1123 E., 2021/645 K.), https://mevzuat.sinerjias.com.tr

Yargıtay 13. Ceza Dairesi, 2019/675 E., 2020/1543 K., https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2016/10781 Karar No: 2017/4966, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8. Ceza Dairesi, Esas No: 2017/897 Karar No: 2017/6019, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2017/1091 Karar No: 2017/12836, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 11.Ceza Dairesi, Esas No: 2017/3943 Karar No: 2019/6476, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 15.Ceza Dairesi, Esas No: 2017/14178 Karar No: 2020/4067, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2017/21566 Karar No: 2020/13171, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2018/1078 Karar No: 2018/2485, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 12.Ceza Dairesi, Esas No: 2018/8586 Karar No: 2019/9340, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 12.Ceza Dairesi, Esas No: 2019/13234 Karar No: 2023/1986, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 2. Ceza Dairesi, Esas No: 2019/1560 Karar No: 2019/8994, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 12..Ceza Dairesi, Esas No: 2020/892 Karar No: 2022/3902, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2020/11243 Karar No: 2023/118, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2020/11287 Karar No: 2023/23, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2020/11457 Karar No: 2023/117, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2020/11515 Karar No: 2021/16487, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2020/12314 Karar No: 2023/2143, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 12.Ceza Dairesi, Esas No: 2021/1911 Karar No: 2021/6594, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 8.Ceza Dairesi, Esas No: 2021/6897 Karar No: 2023/147, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 4.Ceza Dairesi, Esas No: 2021/18163 Karar No: 2023/24635, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 11.Ceza Dairesi, Esas No: 2022/6634 Karar No: 2023/264, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 11.Ceza Dairesi, Esas No: 2023/3092 Karar No: 2023/6122, https://mevzuat.sinerjias.com.tr

T.C. Yargıtay 3.Ceza Dairesi, Esas No: 2023/15137 Karar No: 2024/989, https://mevzuat.sinerjias.com.tr

Yargıtay Ceza Genel Kurulu, Esas No: 2020/1123 Kara No: 2021/645, https://mevzuat.sinerjias.com.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2022/328 , https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2022/774, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2023/426, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2022/925, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2021/1107, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2021/230, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2020/407, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2020/216, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2020/744, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2020/213, https://www.kvkk.gov.tr

Kişisel Verileri Koruma Kurumu, Karar No: 2019/308, https://www.kvkk.gov.tr