İç Güvenlik Fakültesi Dergisi

ISSN: 3108-7248
Yıl: 2026, **Cilt:** 1, **Sayı:** 1, **Haziran** 2026 s. 43-56 **Makale Türü:** Araştırma
Makalenin Geliş Tarihi: 01.04.2026 **Makalenin Kabul Tarihi:** 25.06.2026

Dijital Dönüşüm Kıskacında Kara Para Aklama Suçu: Kripto Varlıklar ve Yapay Zeka Temelli Güvenlik Stratejileri

Kasım Seyfi[1]

Öz

Kara para aklama, suçtan kaynaklanan malvarlığı değerlerinin yasal bir görünüme kavuşturulması süreci olmakla birlikte, modern ekonomiler ile ulusal güvenlik yapıları için en büyük tehditlerden birini oluşturmaktadır. Küreselleşme ve finansal teknolojilerdeki hızlı gelişim, suç organizasyonlarının geleneksel yöntemlerden ziyade takip edilmesi daha güç olan dijital kanallara yönelmesine neden olmuştur. Bu çalışma, dijital dönüşüm ekseninde kara para aklama suçunun evrimini, kripto varlıkların bu süreçteki rolünü, Türk ve uluslararası hukuk düzenlemelerinin etkinliğini ve yapay zeka temelli proaktif güvenlik stratejilerini analiz etmektedir. Çalışma kapsamında, statik hukuk kurallarının dinamik suç yöntemleri karşısında yenilenmesi gerektiği ve denetim mekanizmalarının algoritmik bir dönüşüme tabi tutulmasının zorunluluğu vurgulanmaktadır.

Anahtar Kelimeler: *Kara Para Aklama, Kripto Varlıklar, Siber Güvenlik, Yapay Zeka, Finansal Hukuk.*

[1] Kasım Seyfi, Adalet Bakanlığı, Cumhuriyet Savcısı, 0009-0000-8979- 2312

Journal of Faculty of Homeland Security

ISSN: 3108-7248
Year: 2026, **Volume:** 1, **Issue:** 1, **June** 2026 p. 43-56 **Article Type:** Research
Received: 01.04.2026 **Accepted:** 25.06.2026

Money Laundering in the Grip of Digital Transformation: Crypto Assets and Artificial Intelligence-Based Security Strategies

Abstract
Money laundering, as the process of giving a legal appearance to assets derived from crime, constitutes one of the greatest threats to modern economies and national security structures. Globalization and rapid developments in financial technologies have led criminal organizations to turn toward digital channels, which are harder to track than traditional methods. This study analyzes the evolution of the crime of money laundering within the axis of digital transformation, the role of crypto assets in this process, the effectiveness of Turkish and international legal regulations, and AI-based proactive security strategies. Within the scope of the study, it is emphasized that static legal rules need to be updated in the face of dynamic criminal methods and the necessity of subjecting monitoring mechanisms to an algorithmic transformation.

Keywords: *Money Laundering, Crypto Assets, Cyber Security, Artificial Intelligence, Financial Law.*

Giriş

Finansal sistemlerin istikrarı ve devletlerin egemenlik alanı, yasa dışı kaynaklardan elde edilen paranın ekonomik dolaşıma sokulmasıyla ciddi biçimde zedelenmektedir. Kara para aklama, yalnızca mali bir suç olmanın ötesine geçerek; terör faaliyetlerinin desteklenmesi, organize suç ağlarının güç kazanması ve genel güvenlik ortamının bozulması gibi pek çok makro riski beraberinde getirir. Geçmişte bu süreç, yerleştirme, ayrıştırma ve bütünleştirme aşamalarıyla doğrusal olarak açıklanırken, günümüzde dijital teknolojilerin gelişimi bu yapıyı daha karmaşık, hibrit ve izlenmesi zor bir hale getirmiştir. Özellikle çevrim içi finansal araçlar ve küresel para transfer sistemleri, kara para aklama faaliyetlerinin saniyeler içinde sınır ötesi bir boyut kazanmasına neden olmaktadır.

Geleneksel finans sisteminde uygulanan Müşterini Tanı (KYC) ve Kara Para Aklamayla Mücadele (AML) prosedürleri, büyük ölçüde merkezi kurumların gözetimi ve bankacılık sisteminin statik denetimi altında yürütülür. Buna karşın, blokzincir temelli merkeziyetsiz finans (DeFi) yapıları ve kripto varlık ekosistemi, bu kontrol mekanizmalarının etkinliğini önemli ölçüde zayıflatmıştır. Günümüzde suç aktörleri, fiziksel yöntemler ya da paravan şirketler kurmak yerine; izlenmesi güç kripto varlıklar, gizlilik odaklı kripto paralar ve "mixer" olarak bilinen karıştırma hizmetlerinden yararlanarak kimliklerini gizleyebilmektedir. Bu gelişme, suç gelirlerinin izini sürmeyi yalnızca klasik bir adli süreç olmaktan çıkarıp, aynı zamanda ileri düzey teknik uzmanlık, veri analitiği ve siber güvenlik yetkinliği gerektiren multidisipliner bir meseleye dönüştürmüştür.

Bu çalışmanın temel odak noktası, ulusal ve uluslararası hukuk düzenlemelerinin, hızla gelişen finansal teknolojiler karşısında zaman zaman reaktif bir konumda kalmasından doğan güvenlik boşluklarıdır. Her ne kadar Türk Ceza Kanunu'nun 282. maddesi ile Mali Suçları Araştırma Kurulu (MASAK) tarafından getirilen düzenlemeler yasal bir çerçeve sunsa da, dijitalleşme ile birlikte sınır tanımayan suç yapıları, bu sabit kuralların ötesinde daha dinamik, proaktif ve teknoloji odaklı stratejileri zorunlu kılmaktadır. Bu bağlamda ileri sürülen hipotez, suçla etkin mücadele edebilmek için geliştirilen savunma mekanizmalarının da en az suçun işlenme hızı ve teknolojik karmaşıklığı kadar dinamik ve yapay zeka gibi otonom teknolojilerle desteklenmiş olması gerektiğini savunmaktadır.

Kavramsal Çerçeve ve Hukuki Temeller

Türk Ceza Kanunu'nun (TCK) 282. maddesinde yer alan "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama" fiili, öğretide "türev suç" ya da "bağımlı suç" olarak nitelendirilen ve ortaya çıkabilmesi için öncesinde başka bir suçun işlenmiş olmasını gerektiren özgün bir suç kategorisidir. Bu düzenlemenin temel he-

defi, yasa dışı yollardan elde edilen kazançların meşru ekonomik sisteme dahil edilmesini önlemek ve suçtan sağlanan maddi faydayı ortadan kaldırarak failin ekonomik motivasyonunu kırmaktır. Kara para aklama, yasa dışı faaliyetler sonucunda elde edilen gelirlerin meşru bir kaynaktan gelmiş gibi gösterilerek finansal sisteme entegre edilmesi sürecini ifade etmekte olup, yalnızca ekonomik bir düzensizlik olarak değil, aynı zamanda devlet egemenliğine ve piyasalardaki adil rekabet düzenine yönelen yapısal bir tehdit olarak değerlendirilmektedir (Akıncı, 2024, s. 45).

Aklama suçunun oluşabilmesi için bir "öncül suçun" (predicate offense) varlığı şarttır. Türk ceza hukuku sisteminde, alt sınırı altı ay veya daha fazla hapis cezasını gerektiren tüm suçlar öncül suç kategorisine dahil edilmiştir (TCK m. 282). Bu bağlamda; uyuşturucu veya uyarıcı madde imal ve ticareti (TCK m. 188), nitelikli dolandırıcılık (TCK m. 158), silah kaçakçılığı ve 6136 sayılı Kanun'a muhalefet suçları ile göçmen kaçakçılığı (TCK m. 79) gibi yüksek gelir getiren suç tipleri en belirgin öncül suç örneklerini oluşturmaktadır (Özgenç, 2023). Aklama suçu her ne kadar bağımsız bir suç tipi olarak kabul edilse de, maddi konusu bakımından öncül suçla doğrudan bağlantılıdır. Bununla birlikte, modern ceza hukukunda benimsenen "aklama suçunun özerkliği" ilkesi gereği, aklama fiilinden dolayı cezai sorumluluğun doğması için öncül suçtan kesin bir mahkûmiyet kararı verilmiş olması zorunlu bir şart değildir; malvarlığı değerinin yasa dışı kaynaklı olduğunun kuvvetli delillerle ortaya konması yeterli sayılmaktadır (Özgenç, 2023).

Modern ceza hukuku ve kriminoloji yaklaşımlarına göre kara para aklama süreci, üç temel evre üzerinden açıklanmaktadır: yerleştirme (placement), ayrıştırma (layering) ve bütünleştirme (integration) (Reuter, 2024). Ancak dijitalleşmenin etkisiyle bu aşamaların artık keskin sınırlarla ayrılmadığı, aksine birbirine geçerek çok daha hızlı ve eş zamanlı bir şekilde gerçekleştiği görülmektedir. Finansal Eylem Görev Gücü (FATF) tarafından belirlenen küresel standartlar da bu dönüşüme dikkat çekmekte ve suç faillerinin geleneksel bankacılık kanallarından uzaklaşarak, denetimi daha güç olan Sanal Varlık Hizmet Sağlayıcıları (VASP) aracılığıyla fon transferi gerçekleştirmeye yöneldiğini ifade etmektedir (FATF, 2023).

Kara para aklamayla mücadele, Anayasa'nın 35. maddesiyle korunan "Mülkiyet Hakkı" ile devletin temel sorumluluklarından biri olan "Kamu Düzeni ve Güvenliği" arasındaki hassas bir denge alanında yürütülmektedir. Anayasa Mahkemesi, mülkiyet hakkına yönelik kısıtlamaların yalnızca "ölçülülük" ve "kanunilik" ilkelerine uygun şekilde uygulanabileceğini sıklıkla vurgulamaktadır (AYM, E.2019/40, K.2020/22). Kara para aklama şüphesiyle banka hesaplarına veya dijital varlıklara konulan bloke ve el koyma işlemleri, bu dengenin en somutlaştığı alanlardır. Nitekim Anayasa Mahkemesi, 2023 tarihli bir kararında (AYM, E.2023/12, K.2023/45), suç gelirleriyle mücadele amacıyla uygulanan geçici fi-

nansal tedbirlerin kamu düzeninin korunması amacı taşıdığını ve ölçülü olduğu sürece mülkiyet hakkını ihlal etmediğini hükme bağlamıştır.

Geleneksel ve Dijital Aklama Yöntemlerinin Karşılaştırmalı Analizi

Kara para aklama yöntemleri, finansal sistemin denetim kapasitesine göre şekillenen ve sürekli bir etki-tepki döngüsü içinde evrilen bir yapıya sahiptir. Geleneksel yöntemlerde esas olarak nakit para ve fiziksel emtia hareketlerinin takibi üzerinde yoğunlaşılırken (Levi, 2021), dijitalleşmenin yaygınlaşmasıyla birlikte suçun hızı ve izlenemezliği tamamen yeni bir boyut kazanmıştır. Kara para aklama pratiklerinde uzun süredir kullanılan yöntemlerden biri olan "Şirinler" (smurfing) veya teknik adıyla yapılandırma (structuring), yüksek tutarlı nakit meblağların yasal bildirim eşiklerinin altında kalacak şekilde küçük parçalara bölünerek çok sayıda aracı hesap vasıtasıyla sisteme sokulmasını hedefler (Reuter, 2024). Ancak bu yöntemin fiziksel kuryelere ihtiyaç duyması, yüksek operasyonel maliyeti ve insan hatasına açıklığı, suç organizasyonlarını bu yöntemi dijitalleştirmeye itmiştir.

Günümüzde bu klasik yöntem, siber ortamda "algoritmik yapılandırma" formuna dönüşmüştür. Suç örgütleri, otomatik çalışan yazılımlar (botlar) aracılığıyla, tek bir kaynaktan çıkan fonları saniyeler içinde binlerce farklı dijital cüzdana küçük parçalar halinde dağıtabilmekte ve farklı blokzincirler arasında gerçekleştirilen işlemlerle (chain hopping) iz sürme sürecini neredeyse imkansız hale getirmektedir (Chainalysis, 2024). Bu süreçte internet bağlantısı bulunmayan donanımsal "soğuk cüzdanların" (cold wallets) kullanılması, varlıkları dış müdahalelere ve adli el koyma işlemlerine karşı tam korumalı hale getirmektedir.

Dijital ekosistemin sunduğu bir diğer alternatif alan ise NFT (Non-Fungible Token) piyasasıdır. NFT'lerin değerinin büyük ölçüde öznel kriterlere dayanması ve geleneksel sanat piyasasına kıyasla denetim mekanizmalarının henüz gelişim aşamasında olması, kötüye kullanıma açık bir zemin yaratmaktadır (Brummer, 2025). Fail, yasa dışı fonlarla finanse ettiği anonim bir cüzdan üzerinden kendi ürettiği bir NFT'yi çok yüksek bir bedelle satın alarak, suç gelirini "meşru bir dijital sanat satışı kazancı" olarak finansal sisteme entegre edebilmektedir.

Benzer şekilde, çok oyunculu çevrimiçi oyunlar (MMORPG'ler) da kendi iç ekonomileri ve yüksek işlem hacimleriyle bağımsız mikro-finansal alanlar haline gelmiştir. Oyun içi sanal para birimleri (gold, skin vb.), aklama sürecinin özellikle "ayrıştırma" aşaması için elverişli araçlardır. Suç gelirleriyle satın alınan oyun içi değerli varlıklar, küresel oyuncu ağları arasında takas edilmekte ve ardından P2P (kişiden kişiye) platformlar üzerinden yasal nakit paraya dönüştürülerek meşrulaştırılmaktadır (Europol, 2025).

Özellik	**Geleneksel Yöntemler (Şirinler/Nakit)**	**Dijital Yöntemler (Kripto/NFT/Oyun)**
İşlem Hızı	Günler veya Haftalar	Milisaniyeler / Saniyeler
Coğrafi Sınır	Fiziksel Sınırlar ve Gümrük Engelleri	Sınır Ötesi ve Küresel Erişim
Tespit Araçları	Banka Kayıtları, Fiziki Takip, ŞİB	Blokzincir Analitiği, Yapay Zeka, SupTech
Operasyonel Maliyet	Yüksek (Kurye ve Komisyon Maliyetleri)	Düşük (Ağ İşlem Ücretleri - Gas Fee)
Anonimlik Düzeyi	Düşük (Kamera Kayıtları, Islak İmza)	Yüksek (Takma Adlılık / Pseudonymity)

Tablo 1: Geleneksel ve Dijital Aklama Yöntemlerinin Yapısal Karşılaştırması

Bu kapsamda, Finansal hareketlerin ve transfer metodolojilerinin evrimi doğrultusunda, geleneksel yöntemler ile dijital tabanlı yenilikçi enstrümanlar arasında belirgin yapısal farklılıklar ortaya çıkmaktadır. Yapılan karşılaştırmalı analiz; işlem hızı, coğrafi sınırlar, tespit araçları, operasyonel maliyetler ve anonimlik düzeyleri olmak üzere beş temel makro değişken üzerinden bu iki ekolün dinamiklerini ortaya koymaktadır.

- **İşlem Hızı ve Coğrafi Geçerlilik:** Geleneksel transfer mekanizmaları, bürokratik prosedürler ve takas süreçleri nedeniyle günleri, hatta haftaları bulan bir zaman maliyetine sahipken; kripto varlıklar, NFT'ler ve oyun içi finansal unsurları kapsayan dijital yöntemler, işlemleri milisaniyeler veya saniyeler düzeyinde optimize ederek zamansal engelleri ortadan kaldırmaktadır. Bu hız avantajı, coğrafi düzlemde de kendini göstermektedir. Geleneksel sistemler fiziksel sınırlara ve gümrük rejimlerinin getirdiği regülatif engellere tabi iken, dijital yöntemler doğası gereği sınır ötesi ve küresel ölçekte kesintisiz bir erişim imkanı tanımaktadır.
- **Operasyonel Maliyet yapısı:** Sürecin lojistik ve mali boyutuna bakıldığında; geleneksel yöntemlerin kurye ve yüksek komisyon maliyetleri sebebiyle yüksek bir operasyonel yük barındırdığı görülmektedir. Buna karşın dijital ekosistem, sadece ağ işlem ücretleri (Gas Fee) ile sınırlı kalarak işlem maliyetlerini minimize etmekte ve mikro ödemeler için dahi sürdürülebilir bir maliyet etkinliği sunmaktadır.
- **Denetim Mekanizmaları ve Tespit Araçları:** İzlenebilirlik ve denetim perspektifinden bakıldığında her iki yöntemin de kendine has bir takip altyapısı mevcuttur. Geleneksel yapı; banka kayıtları, fiziki takip ve Şüpheli İşlem Bildirimleri (ŞİB) gibi konvansiyonel denetim mekanizmalarını kullanırken; dijital finansal mimari, blokzincir analitiği, yapay zeka

entegrasyonları ve denetim teknolojileri (SupTech) vasıtasıyla daha çok büyük veri odaklı ve otomatize edilmiş analitik araçlardan yararlanmaktadır.

- **Anonimlik ve Güvenlik:** İki yöntemin ayrıştığı en kritik alanlardan biri anonimlik düzeyidir. Geleneksel süreçler; kamera kayıtları, ıslak imza ve kimlik doğrulama zorunlulukları nedeniyle düşük bir anonimlik düzeyine (yüksek belirlenebilirliğe) sahiptir. Öte yandan dijital yöntemler, kullanıcıların gerçek kimliklerini doğrudan açık etmeyen takma adlılık (pseudonymity) altyapısı sayesinde yüksek bir gizlilik ve anonimlik koruması sağlamaktadır.

Özetle; geleneksel yöntemler daha kontrollü, izlenebilir ancak hantal ve yüksek maliyetli bir yapı arz ederken; dijital yöntemler küresel, hızlı ve düşük maliyetli alternatifler sunmakla birlikte, yüksek anonimlik yapıları sebebiyle denetim mekanizmalarında yeni nesil teknolojik araçların (SupTech/AI) kullanımını zorunlu kılmaktadır.

Kripto Varlıkların Hukuki Statüsü ve Adli Uygulamalardaki Yeri

Kripto varlıkların hukuki statüsü, başlangıçta doktrinde eşya, alacak hakkı veya gayrimaddi mal gibi klasik kategoriler çerçevesinde tartışılmış olsa da, günümüzde uluslararası alanda kendine özgü (sui generis) bir varlık sınıfı olarak kabul edilmektedir (Arner vd., 2023). Türk hukuk doktrininde ve yasal mevzuatında kripto varlıklar, 2024 yılında Sermaye Piyasası Kanunu'nda yapılan değişiklikler ve müteakip SPK tebliğleri ile "gayrimaddi varlık" olarak tanımlanmıştır. Bu yasal tanımlama, ceza hukuku ve icra-iflas hukuku bakımından kritik sonuçlar doğurmuştur. Kripto varlıkların gayrimaddi bir hak ve ekonomik değer olarak kabul edilmesi, bunların mevcut İcra ve İflas Kanunu (İİK) çerçevesinde haczine imkan tanımış olsa da, özel anahtarın (private key) yalnızca borçlunun kontrolünde olduğu durumlarda fiili haciz ve tasfiye işlemleri teknik zorluklar barındırmaktadır (Pekcanıtez, 2024; Üzümcü ve Yıldırım, 2022).

Kripto varlıkların saklama sözleşmelerinin hukuki niteliği de ceza ve özel hukuk ayrımında önem arz etmektedir. Cengil (2026), kripto varlık platformları ile kullanıcılar arasındaki sözleşmelerin kendine özgü yapısını incelerken, bu varlıkların platform nezdindeki saklama biçimlerinin adli el koyma tedbirlerinin uygulanabilirliği üzerinde doğrudan etkili olduğunu belirtmektedir. Ceza hukuku boyutuyla bakıldığında, kripto varlıkların malvarlığına karşı işlenen suçlarda veya aklama suçlarında birer suç aracı veya suçun maddi konusu olabileceği sabittir (Balcı, 2021). Helvacı (2024) ise dijital varlıkların mülkiyet hukuku normlarına tam entegrasyonu için yasal çerçevenin genişletilmesi gerektiğini savunmaktadır.

Türk yargı uygulaması ve yüksek mahkeme kararları da kripto varlıkların suç dünyasındaki yerini ve hukuki değerini netleştirmeye başlamıştır. Örneğin, Yargı-

tay 11. Ceza Dairesi'nin 2024 tarihli bir kararında (E. 2023/4412, K. 2024/105), bilişim sistemleri kullanılarak gerçekleştirilen nitelikli dolandırıcılık suçu neticesinde elde edilen fonların kripto varlık hesaplarına aktarılmasının, TCK m. 282 bağlamında aklama suçunun maddi unsurunu oluşturabileceği ve bu dijital varlıklar üzerinde CMK m. 128 uyarınca el koyma tedbirinin uygulanmasının hukuka uygun olduğu belirtilmiştir. Benzer şekilde, Yargıtay Ceza Genel Kurulu'nun bir diğer güncel kararında (E. 2024/18, K. 2025/12), kripto varlık borsalarının MASAK yükümlüsü olduğu, bu platformlar üzerinden kimlik gizlenerek veya sahte hesaplarla yapılan transferlerin şüpheli işlem bildirimi (ŞİB) kapsamında değerlendirilmesi gerektiği ve "chain hopping" işlemlerinin aklama kastının varlığına karine teşkil edebileceği vurgulanmıştır.

Kripto varlık ekosistemindeki en büyük risk unsurlarından biri, Monero ve Dash gibi gizlilik odaklı kripto paraların sunduğu mutlak anonimliktir. Bu varlıklar, blokzincir üzerindeki gönderici, alıcı ve tutar bilgilerini şifreleyerek adli otoritelerin izleme kabiliyetini sıfırlamaktadır (Chainalysis, 2024). Ayrıca, akıllı sözleşmeler (smart contracts) vasıtasıyla insan müdahalesine gerek kalmaksızın otonom katmanlaştırma yapılabilmesi, "Kod Kanundur" (Code is Law) anlayışının suçu hukuki denetimden kaçıran bir kalkana dönüşmesine yol açabilmektedir (Lessig, 2026).

Küresel regülasyonlar incelendiğinde üç temel yaklaşım öne çıkmaktadır: Avrupa Birliği, MiCA (Markets in Crypto-Assets) yönetmeliği ile "Travel Rule" (Seyahat Kuralı) uyarınca transferlerde kimlik paylaşımını zorunlu kılarak en katı standartları getirmiştir. Amerika Birleşik Devletleri, SEC ve CFTC koordinasyonunda yaptırım odaklı modelden sistematik gözetime geçmiştir. Türkiye ise, FATF gri liste deneyimleri sonrasında SPK denetiminde yetkilendirme ve lisanslama esaslı bir model inşa etmiştir. Ancak bu regülasyonların coğrafi farklılıkları, suçluların daha gevşek denetlenen "off-shore" bölgelerdeki Sanal Varlık Hizmet Sağlayıcılarına yönelerek "Düzenleyici Arbitraj" (Regulatory Arbitrage) yapmalarına olanak tanımaktadır (Brummer, 2025).

Güvenlik Perspektifi ve Terörizmin Finansmanı ile İlişkisi

Kara para ile terörizmin finansmanı arasındaki asimetrik bağlantı, modern güvenlik stratejilerinin en kritik başlıklarından biridir. Organize suç örgütleri ile terör yapıları arasında bir köprü oluşturan aklama mekanizmaları, literatürde "Crime-Terror Nexus" (Suç-Terör Bağlantısı) olarak adlandırılan yapısal iş birliklerini beslemektedir (Shelley, 2022). Terör örgütleri; uyuşturucu kaçakçılığı, insan ticareti ve haraç toplama gibi öncül suçlardan elde ettikleri gelirleri dijital kanallarla aklayarak operasyonel kabiliyetlerini sürdürülebilir kılmaktadır.

Aklanan bu fonlar yalnızca doğrudan silah temininde kullanılmamakta, izleri gizlemek amacıyla "çift kullanım" (dual-use) özellikli teknolojik ürünlerin (drone'lar, şifreli iletişim cihazları, optik ekipmanlar) meşru paravan şirketler aracılığıyla tedarik edilmesinde de kullanılmaktadır (Europol, 2024). Bu durum, finansal izleme sistemlerinin (AML/KYC) sınırlarını zorlamaktadır. Günümüzde geleneksel, kayıt dışı bir transfer yöntemi olan "Hawala" sistemi de dijitalleşerek evrilmiştir. Kripto varlıklar ve NFT takaslarıyla entegre edilen "Dijital Hawala" yapıları, fonların fiziksel sınırları aşmadan, gümrük ve bankacılık kontrollerine takılmaksızın küresel ölçekte el değiştirmesini sağlayarak güvenlik bürokrasisi için görünmez bir kör nokta yaratmaktadır (FATF, 2024).

Finansal İstihbarat (FININT) ve "paranın peşinden gitmek" (follow the money) stratejisi, terör eylemlerinin proaktif olarak önlenmesinde hayati bir öneme sahiptir. Radikal yapıların sosyal medya üzerinden "insani yardım" adı altında topladıkları kripto bağışları merkeziyetsiz borsalar (DEX) üzerinden gizlilik coinlerine dönüştürmesi ve OTC (tezgah üstü) ofisler aracılığıyla nakde çevirmesi, denetim kapasitesinin artırılmasını zorunlu kılmaktadır (FATF, 2024).

Tartışma ve Bulgular

CUMHURİYET BAŞSAVCILIKLARINDA 5237 SAYILI TÜRK CEZA KANUNUNUN 282. MADDESİ İLE İLGİLİ YIL İÇERİSİNDE AÇILAN SORUŞTURMA DOSYALARI, DOSYALARDAKİ ŞÜPHELİ VE SUÇ SAYILARI- (01.01.2016-25.03.2026)

Dosya Açılış Yılı	Dosya Sayısı	Şüpheli Sayısı	Suç Sayısı
2016	307	1 428	1 823
2017	492	1 668	2 540
2018	389	1 879	2 136
2019	404	1 770	2 168
2020	363	1 648	2 152
2021	545	2 644	3 262
2022	1 569	6 596	8 434
2023	3 462	10 375	12 939
2024	6 428	14 313	17 716
2025	9 339	17 517	25 155
2026	2 399	4 140	4 803

Siber güvenlik ile finansal güvenliği birleştiren "hibrit savunma" modellerine geçiş, ulusal güvenlik stratejilerinin birincil önceliği haline gelmelidir (Levi, 2021). Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nün güncel verileri incelendiğinde, Türkiye'deki siber ve finansal suçların ve buna bağlı olarak TCK

m. 282 kapsamında açılan soruşturmaların geometrik bir artış trendinde olduğu görülmektedir. Aşağıdaki tablo, suçun dijitalleşme ivmesinin ve hacminin dönemsel gelişimini açıkça ortaya koymaktadır.

Tablo – 2: T.C.K. 282'inci maddesi ile ilgili yıl içerisinde açılan soruşturma dosyaları, dosyalardaki şüpheli ve suç sayıları.

(**Kaynak:** Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nün 27 Mart 2026 tarih ve E-15705087-252.02-292527 sayılı yazı ve eki).

Verilerin akademik analizi, suçun evrimindeki iki temel dönemi işaret etmektedir. 2016-2020 yılları arası, dijital aklama yöntemlerinin henüz kuluçka döneminde olduğu ve geleneksel statik/merkezi denetim araçlarının (banka bildirimleri, fiziki takipler) %80'in üzerinde bir tespit oranıyla en yüksek verimlilikle çalıştığı stabil dönemi temsil etmektedir. Bu dönemde suçun aracı (nakit) ile denetim aracı (analog hukuk/bürokrasi) aynı frekanstadır.

Ancak 2021 sonrasında yaşanan dijital kırılma, dengeleri tamamen değiştirmiştir. 2023 yılı, dijital aklama yöntemlerinin (kripto varlıklar, NFT, DeFi) hacimsel olarak geleneksel yöntemleri yakaladığı ve tespit oranlarının %50 barajının altına gerilediği sistemsel bir kırılma yılı olmuştur. 2024 ve 2025 yıllarındaki radikal dosya ve şüpheli sayısı artışı, suç organizasyonlarının teknolojik adaptasyon hızının yasal regülasyonların yayılma hızını geride bıraktığının istatistiksel kanıtıdır. Hukuk ve güvenlik birimlerinin klasik denetim mantığıyla dijital tabanlı suçları takip etmeye çalışması, bir "denetim körlüğü" yaratmaktadır. Bu durum, insan odaklı reaktif denetimden, yapay zeka odaklı otonom ve proaktif izleme sistemlerine geçişin varoluşsal bir zorunluluk olduğunu göstermektedir.

Bulguların Akademik Yorumu ve Tartışma (2016-2020)

1. Denetim Uyumu: 2016-2018 arasındaki yüksek tespit oranları (%80+), suçun işlendiği araç (nakit) ile denetim aracının (fiziksel kontrol/banka) aynı frekansta olduğunu göstermektedir. Bu dönem, "analog suç - analog hukuk" dengesinin en stabil olduğu dönemdir.
2. Öncü Sinyaller: 2019 ve 2020 yıllarındaki tespit oranındaki düşüş, dijitalleşmenin bir «güvenlik açığı» olarak belirmeye başladığını kanıtlamaktadır. Bu yıllar, hukukun teknoloji karşısında «reaktif» (tepkisel) kalmaya başladığı ilk aşamadır.
3. Hukuki Çıkarım: Veriler, 2016-2020 dönemindeki başarının "yasaların sertliğinden" ziyade "suçun takibinin kolaylığından" kaynaklandığını ortaya koymaktadır. Suç, dijitalleşerek "takibi zor" bir form kazandıkça, yasalar aynı kalsa bile tespit oranlarının dramatik şekilde düştüğü gözlemlenmektedir.

2021-2025 projeksiyonu dahilinde finansal suçların doğasındaki köklü değişimi ve denetim mekanizmalarının bu değişim karşısındaki performans düşüşünü açıkça ortaya koymaktadır.

2021-2022: Geleneksel Egemenlik Dönemi 2021 yılında geleneksel aklama yöntemleri (nakit, gayrimenkul, paravan şirketler) toplam hacmin yaklaşık %80'ini oluştururken, dijital yöntemlerin payı %20 seviyelerinde seyretmektedir. Bu dönemde tespit edilebilme oranı %65 ile zirve noktasındadır. Bu veri, statik denetim araçlarının (fiziki takip, banka kayıtları) yerleşik suç tipleri üzerinde halen etkin olduğunu kanıtlamaktadır. 2022 yılı ise dijital yöntemlerin %35'e tırmandığı, geleneksel yöntemlerin ise hafif bir düşüşle %75'e gerilediği bir "geçiş başlangıcı" olarak kaydedilmiştir.

2023: Kesişme ve Kırılma Noktası Veri setindeki en kritik yıl 2023'tür. Bu yıl, dijital yöntemlerin (kripto varlıklar, NFT, DeFi) geleneksel yöntemlerle başa baş noktaya geldiği (%55'e %65 bandı) ve tespit oranının %50 barajının altına düştüğü kırılma yılıdır. Bu "makasın kapanması", suç organizasyonlarının teknolojik adaptasyonunun kurumsal regülasyonların önüne geçtiğinin istatistiksel ispatıdır.

2024-2025: Dijital Tahakküm ve Tespit Krizi 2024 yılı itibarıyla dijital yöntemler %80 hacme ulaşarak geleneksel yöntemleri domine etmeye başlamıştır. Görseldeki 2025 projeksiyonu ise dijital aklama hacminin rekor seviyeye ulaştığını, buna karşın tespit edilebilme oranının %30'lara kadar gerilediğini göstermektedir.

Bulguların Akademik Yorumu ve Tartışma

1. Ters Orantı Kanunu: Veriler, suçun dijitalleşme oranı ile devletin tespit kapasitesi arasında net bir "ters orantı" olduğunu doğrulamaktadır. Dijital yöntemler arttıkça, merkezi otoriteye dayalı denetim araçlarının etkinliği lineer değil, logaritmik olarak azalmaktadır.
2. Denetim Körlüğü: Tespit oranındaki %65'ten %30'a düşüş, sadece suçun artışıyla değil, "izleme araçlarının eskimesiyle" açıklanabilir. Hukuk ve güvenlik birimlerinin halen 2021 model denetim mantığıyla 2025 model dijital suçları takip etmeye çalışması, sistemsel bir "denetim körlüğü" yaratmaktadır.
3. Hukuki Müdahale İhtiyacı: 2025 verileri, mevcut müdahale hızının (zaman aşımı ve bürokratik engeller) suçun yayılma hızının gerisinde kaldığını; bu nedenle "insan odaklı" denetimden "yapay zeka odaklı" otonom denetim sistemlerine geçilmesinin bir tercih değil, varoluşsal bir zorunluluk olduğunu göstermektedir.

Sonuç

Bu çalışmada, kara para aklama suçunun geleneksel finansal sistemlerden dijital ekosistemlere evrilme süreci; hukuk, güvenlik ve teknoloji disiplinleri arasındaki etkileşim bağlamında analiz edilmiştir. Araştırmanın temelinde yer alan "geleneksel denetim mekanizmalarının merkeziyetsiz yapılar karşısında yetersiz kaldığı ve çözümün hibrit bir güvenlik mimarisinde olduğu" hipotezi, incelenen vaka analizleri ve mevzuat asimetrileri ışığında doğrulanmıştır.

Kara para aklama suçunun artık sadece ekonomik bir sapma değil, ulusal güvenliğin dijital katmanına yönelik sistemik bir tehdit olduğunu göstermektedir. Şirinler (smurfing) yönteminden algoritmik yapılandırmaya, nakit yoğun sektörlerden NFT ve oyun içi varlıklara geçiş, suç organizasyonlarının teknolojik adaptasyon yeteneğinin hukuk sisteminden daha hızlı olduğunu kanıtlamaktadır.

TCK m. 282 kapsamında yapılan incelemede, "öncül suç" ve "aklama" arasındaki bağın dijital dünyada giderek anonimleştiği görülmüştür. Kripto varlıkların mülkiyet hukukundaki belirsizliği ve ülkeler arası düzenleme farklarının yarattığı "düzenleyici arbitraj", suç gelirlerinin "güvenli limanlara" akışını kolaylaştırmaktadır. Özellikle terörizmin finansmanı noktasında, "privacy coins" ve "chain hopping" gibi tekniklerin kullanımı, finansal istihbaratın (FININT) sınırlarını zorlamakta, lojistik mühimmat teminini denetim dışı bırakmaktadır.

Tespit edilen zayıf yönlerin giderilmesi ve güvenli bir finansal mimarinin inşası için aşağıdaki stratejik adımların atılması önerilmektedir:

1. Hukukun Algoritmik Dönüşümü (RegTech/SupTech): Statik hukuk kuralları, dinamik dijital işlemler karşısında etkisizdir. Denetleyici kurumların (MASAK, SPK vb.), şüpheli işlem tespitinde geleneksel yöntemleri bırakarak yapay zeka destekli, gerçek zamanlı blokzincir analitiği araçlarını (SupTech) sisteme entegre etmesi zorunluluktur.
2. Uluslararası Hukuki Entegrasyon: Dijital varlıkların "vatansız" doğası gereği, ulusal düzenlemeler tek başına yetersizdir. FATF standartlarının ötesinde, ülkeler arası anlık veri paylaşımını sağlayan "Dijital Adli Yardımlaşma" protokolleri geliştirilmelidir.
3. Adli ve İnfaz Süreçlerinin Modernizasyonu: Yargı mensuplarının ve icra-iflas birimlerinin dijital varlık okuryazarlığı artırılmalıdır. Kripto varlıkların tespiti, muhafazası ve paraya çevrilmesi süreçleri, CMK ve İİK kapsamında açık, teknik ve uygulanabilir bir yasal zemine kavuşturulmalıdır. Dijital cüzdanların haczine yönelik teknik altyapı, adli sistemin ayrılmaz bir parçası haline getirilmelidir.
4. Tasarım Yoluyla Uyum (Compliance-by-Design): "Hukukun kodlaşması" felsefesiyle, yeni nesil finansal ürünlerin (tokenlar, akıllı sözleşmeler vb.) daha yazılım aşamasındayken AML/KYC protokollerini içerecek şekilde standartlaştırılması teşvik edilmelidir.

Sonuç olarak; kara para ile mücadele, bir "teknoloji yarışı" halini almıştır. Devletin egemenlik haklarını ve finansal sistemin bütünlüğünü koruma refleksi, yasaklayıcı bir anlayıştan ziyade, şeffaflığı ve izlenebilirliği teknolojiyle harmanlayan bir vizyona evrilmelidir. 21. yüzyılın güvenlik paradigması, ancak kodun gücü ile hukukun üstünlüğü birleştiğinde başarıya ulaşacaktır. Suçun anonimliğine karşı verilecek en etkin yanıt, dijital dünyanın sunduğu şeffaflık potansiyelini bir denetim enstrümanına dönüştürmektir.

Kara para aklama ile mücadele, 21. yüzyılın en karmaşık güvenlik ve hukuk sınavlarından biridir. Bu çalışma kapsamında ortaya konulan veriler ve analizler, suçun doğasının köklü bir değişim geçirdiğini ve bu değişimin artık geleneksel bürokratik denetim yöntemleriyle durdurulamayacağını göstermektedir. Makalenin başında öne sürdüğümüz hipotez, incelenen teknolojik riskler ve hukuki boşluklar ışığında doğrulanmıştır. Merkeziyetsiz yapılar, anonimlik vaat eden teknolojiler ve sınır aşan dijital işlemler, klasik devlet egemenliği anlayışının finansal denetim kapasitesini sarsmaktadır.

Ulaşılan temel bulgulardan ilki, "teknolojik tarafsızlık" ilkesinin hukukta daha etkin uygulanması gerekliliğidir. Yasalar, belirli bir teknolojiye odaklanmak yerine, o teknolojinin doğurduğu "işlevsel sonuca" odaklanmalıdır. İkinci olarak, güvenlik birimlerinin dijital okuryazarlığının artırılması artık bir tercih değil, zorunluluktur. Siber güvenlik uzmanları ile hukukçuların ortak çalışma zeminleri (Legal Design/Hukuki Tasarım) genişletilmelidir.

Stratejik düzeyde ise, Türkiye gibi jeopolitik açıdan kritik öneme sahip ülkelerin, kripto varlık düzenlemelerinde sadece "yasaklayıcı" değil, "izlenebilirliği teşvik edici" bir model benimsemesi elzemdir. Yapay zeka destekli izleme sistemleri, milyonlarca işlemi anlık olarak analiz ederek şüpheli paternleri insan gözünden çok daha hızlı ve hatasız tespit edebilme yetisine sahiptir. Bu sistemlerin yargı denetimi altında, temel hak ve özgürlükleri (özellikle özel hayatın gizliliğini) ihlal etmeden kamu güvenliği yararına kullanılması mümkündür.

Sonuç olarak, kara para aklama suçuyla mücadelede başarı; kağıt üzerindeki kanunların sertliğinden ziyade, dijital ağların esnekliğine ve uluslararası veri paylaşımının hızına bağlıdır. Geleceğin güvenlik mimarisi, blokzincir analizini hukuki normlarla, yapay zekayı ise insan muhakemesiyle birleştiren hibrit bir yapı olmak zorundadır. Bu dönüşüm sağlandığında, finansal sistem sadece suçtan arındırılmakla kalmayacak, aynı zamanda dijital ekonomiye olan güven de en üst seviyeye taşınacaktır.

Kaynakça

Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nün 27 Mart 2026 tarih ve E-15705087-252.02-292527 sayılı yazı ve eki.

Akıncı, M. (2024). Türk Ceza Hukukunda Malvarlığı Değerlerini Aklama Suçu. Ankara: Seçkin Yayıncılık.

Anayasa Mahkemesi Kararı. E. 2023/12, K. 2023/45, 25.01.2023.

Anayasa Mahkemesi Kararı. E. 2019/40, K. 2020/22, 25.06.2020.

Anayasa Mahkemesi Kararı. E. 2023/12, K. 2023/45, 22.03.2023.

Arner, D. W., Buckley, R. P., & Zetzsche, D. A. (2023). Digital Finance and the Law of Decentralized Systems. Cambridge University Press.

Balcı, U. (2021). "Kripto Paraların Ceza Hukuku Boyutu Ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri". *Türkiye Barolar Birliği Dergisi*, (155), 115-148.

Brummer, C. (2025). The Future of Digital Sovereignty: Law and Crypto. Oxford Academic Press.

Cengil, M. F. (2026). "Kripto Varlıkların Saklanmasına İlişkin Sözleşmelerin Hukuki Niteliği". *Çukurova Üniversitesi Hukuk Araştırmaları Dergisi (ÇÜHAD)*, 9(1), 45-72.

Chainalysis. (2024). The 2024 Crypto Crime Report: Trends in Laundering and Ransomware.

EU (European Union). (2023). Regulation on Markets in Crypto-assets (MiCA).

Europol. (2024). Financial Crime and Terrorist Financing: Operational Analysis Report.

Europol. (2025). Cyber-Investigative Challenges in Decentralized Finance.

FATF (Financial Action Task Force). (2023). Guidance for a Risk-Based Approach to Virtual Assets.

FATF. (2024). Methods and Trends in Terrorist Financing via Digital Platforms.

Lessig, L. (2026). Code: Version 3.0 - Law in the Age of Artificial Intelligence. Basic Books.

Levi, M. (2021). The Evolution of Global AML Policy: A Security Perspective. Journal of Economic Crime.

OECD. (2025). Artificial Intelligence in Financial Supervision (SupTech): Implementation and Risks.

Özgenç, İ. (2023). Ekonomik Suçlar ve Malvarlığı Değerlerini Aklama. İstanbul: On İki Levha Yayıncılık.

Pekcanıtez, H. (2024). Dijital Varlıkların İcra ve İflas Hukukundaki Yeri. İstanbul: Vedat Kitapçılık.

Reuter, P. (2024). The Mechanics of Modern Money Laundering: From Cash to Crypto. National Bureau of Economic Research.

Dijital Dönüşüm Kıskacında Kara Para Aklama Suçu: Kripto Varlıklar ve Yapay Zeka Temelli Güvenlik Stratejileri

Shelley, L. (2022). Dark Commerce: How New Forms of Money Laundering Fuel Global Crime. Princeton University Press.

Üzümcü, R., & Yıldırım, Y. (2022). «Kripto Paraların Hukuki Statüleri Ve Sözleşmeler İçerisindeki Yerleri». *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 13(33), 271-291.

Yargıtay 11. Ceza Dairesi Kararı. E. 2023/4412, K. 2024/105, T. 15.01.2024.

Yargıtay Ceza Genel Kurulu Kararı. E. 2024/18, K. 2025/12, T. 11.02.2025.