TAAD Yıl 17 . Sayı 68 . Ekim 2026
ISSN 1309-6826 - E-ISSN 3150-0919
Araştırma Makalesi/Research Article DOI: 10.54049/taad.1950436

# BİLİŞİM SİSTEMLERİ VASITASIYLA İŞLENEN ISRARLI TAKİP SUÇU: TEKNOLOJİK SORUNLAR VE REFORM ÖNERİLERİ

*The Stalking Crimes Committed Through Information Systems: Technological Problems and Reform Proposals*

**İbrahim KORKMAZ***

## Özet

Israrlı takip, mağdurun rızası olmadan sürekli olarak devam eden ve mağdurun yaşam alanını sistematik bir şekilde kuşatarak psikolojik baskı oluşturan bir davranış biçimidir. Günümüzde, bilişim sistemlerinin sağladığı anonimlik ve mekândan bağımsızlık sayesinde, mağdur üzerinde kesintisiz bir siber şiddet uygulanabilmektedir. Bu çalışma, TCK m. 123/A'da düzenlenen ısrarlı takip suçunun işlenme türlerinden biri olan bilişim sistemleri vasıtasıyla işlenen ısrarlı takip suçunu kavramsal ve teorik temelleriyle incelemeyi, benzer suç ve eylemlerden (TCK m. 123, 105, 106, 134; mobbing; siber zorbalık; spam) farklarını göstermeyi, yeni dijital uygulamalar (doxxing, rıza dışı ifşa/intikam pornosu, deepfake taciz) ve teknoloji temelli araçların (botlar, GPS ve stalkerware, IoT, Metaverse/VR) yarattığı çeşitli sorunları inceleyerek Türk hukuku için reform ihtiyacını ortaya koymayı amaçlamaktadır. Mağdurun hem fiziksel hem de dijital huzur ve güvenliğini sağlamak amacıyla, bilişim sistemleri vasıtasıyla takip için TCK m. 123'ten ayrı, özgün bir düzenleme yapılması veya TCK m. 123/A'da yer alan "temas" kavramının izleme ve gözetlemeyi de içerecek şekilde genişletilmesi, "fiziken takip" teriminin teknolojik dolaylı takip ve sanal alanları kapsayacak şekilde güncellenmesi, yapay zekâ, bot, deepfake gibi yöntemler için özel dijital uzaklaştırma ve erişim yasakları düzenlenmesi, platform iş birliği ve dijital delil standartlarının güçlendirilmesi; bütüncül bir ceza politikası oluşturmak için çalışmamızda teklif edilen reform önerilerini oluşturmaktadır.

**Anahtar kelimeler:** Israrlı takip suçu, bilişim sistemleri, siber şiddet, dijital ayak izleri, dijital deliller

## Abstract

Stalking is a form of behavior that continues uninterrupted without the victim's consent, systematically encircling the victim's living space and creating psychological pressure. Today, thanks to the anonymity and geographical independence provided by information systems, uninterrupted cyberviolence can be inflicted on the victim. This study aims to examine the crime of stalking committed through information systems, one of the types of stalking regulated in Article 123/A of the Turkish Penal Code, from its conceptual and theoretical foundations; to demonstrate its differences from similar crimes and actions (Articles 123, 105, 106, 134 of the Turkish Penal Code; mobbing; cyberbullying; spam); and to highlight the need for reform in Turkish law by

- *Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.*
- *Makale Geliş Tarihi/Article Received Date: 15.4.2026*
- *Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 17.7.2026*

* Dr. Öğr. Üyesi, İstanbul Beykent Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Ana Bilim Dalı, İstanbul/Türkiye, e-posta: ibrahimkorkmaz@beykent.edu.tr, https://orcid.org/0000-0002-5690-432X

examining the various problems created by new digital applications (doxxing, non-consensual disclosure/revenge pornography, deepfake harassment) and technology-based tools (bots, GPS and stalkerware, IoT, Metaverse/VR). The study also aims to address the need for reform in Turkish law regarding stalking through information systems, in order to ensure the physical and digital peace and security of the victim. The proposed reforms in our study to create a holistic criminal policy include; creating a separate, original regulation from Article 123; expanding the concept of "contact" in Article 123/A of the Turkish Penal Code to include monitoring and surveillance; updating the term "physical tracking" to encompass technological indirect tracking and virtual spaces; regulating specific digital removal and access restrictions for methods such as artificial intelligence, bots, and deepfakes; and strengthening platform cooperation and digital evidence standards.

**Keywords:** Stalking crime, information systems, cyber violence, digital footprints, digital evidence

## GİRİŞ

Israrlı takip (stalking), bir kimsenin rızası dışında gerçekleştirilen, süreklilik arz eden ve mağdurun yaşam alanını sistematik bir şekilde kuşatarak mağdur üzerinde psikolojik baskı kuran bir davranışlar bütünüdür.[1] Bu fiiller, zaman içinde tekrarlanarak ve belirli bir "ısrar" iradesiyle birleşerek, mağdurun ciddi bir huzursuzluk hissetmesine, güvenlik endişesi taşımasına ve sonucunda yaşam tarzını değiştirmek zorunda kalmasına neden olabilecek yoğunluğa erişebilir.[2] Geleneksel olarak fiziksel takip ve doğrudan temas kurma çabalarıyla tanımlanan bu suç türü, günümüzde bilişim sistemlerinin sunduğu olanaklar sayesinde, mekândan bağımsız, anonim ve kesintisiz bir siber şiddet biçimine dönüşerek bireyin özel hayatının gizliliğini ve hareket özgürlüğünü sürekli tehdit edebilir hale gelmiştir.[3]

Israrlı takip (stalking) eylemi, bir suç olmanın ötesinde, temelinde karmaşık psikolojik dinamikler ve sosyolojik çatışmalar barındıran davranışlar bütünüdür. İnsanların neden bir başkasını sistematik olarak takip ettiklerine dair yapılan araştırmalar, bu motivasyonun nadiren tek bir nedene dayandığını; çoğunlukla güç, kontrol, saplantı ve reddedilme duygularının bir bileşimi olduğunu göstermiştir.[4] Israrlı takip suçunu işleyen kişileri inceleyen araştırmalar, en yaygın fail tipinin "reddedilmiş takipçi" olduğunu *gö*stermektedir.[5] Bu tip vakalarda fail, biten

---

1 Ayşenur Cihan, 'Türk Ceza Hukuku Bağlamında Israrlı Takip Suçu (TCK Md. 123_A)' (2023) 13 Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi 339; Murat Volkan Dülger, 'Normatif Düzenleme Açısından Israrlı Takip Suçu' (2023) 8 İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 21; Sezgi Demirkale, 'Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Hasan Kalyoncu Üniversitesi 2024) 7.

2 Murat Balcı ve Kerim Çakır, 'Israrlı Takip Suçu (TCK m. 123/A)' (2022) 10 Kadir Has Üniversitesi Hukuk Fakültesi Dergisi 323.

3 Elif Gizem Gündoğdu, 'Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2025); Ayşe Güneş, 'As a Continuity of the Different Forms of Violence: Gender-Based Digital Violence Against Women' (2024) 5 Sosyal Mucit Academic Review 118 https://doi.org/10.54733/smar.1440636 (Erişim tarihi: 6 Mayıs 2026).

4 Cihan (n 1) 342; Nedim Havle, 'Israrın Psikolojik Anatomisi: Yargıtay İçtihatları Işığında TCK Madde 123'ün Sübjektif Unsurları' (2025) 7 Adli Bilimler ve Suç Araştırmaları Dergisi 221.

5 Havle (n 4) 233.

bir ilişkinin ardından duyduğu öfke veya ayrılığı kabullenememe haliyle, takip eylemini kaybettiği kontrolü yeniden kazanmanın bir yolu olarak kullanmaktadır.[6] Mağduru sürekli izlemek, onun yaşamına dair her ayrıntıya vakıf olmak ve mağdurun yaşam tarzını değiştirmesine yol a*çacak derecede bir korku atmosferi oluşturmak, fail için bir* "hükmetme" aracı haline gelmektedir.[7]

Diğer yandan, ısrarlı takibin arkasındaki motivasyon her zaman geçmiş bir ilişkiye olmayabilir. Bazı vakalarda fail, mağdurla arasında hiçbir bağ olmamasına rağmen, "erotomania" olarak adlandırılan ve mağdurun kendisine *âşık* olduğu yönündeki hayali inançlarla hareket edebilmektedir.[8] Bu tür "yakınlık arayan" failler için takip, hayali bir aşkı gerçeğe dönüştürme çabasıyken; "yetersiz takipçi" olarak tanımlanan bir diğer grup için ise takip etmek, sosyal beceri eksikliğini telafi etmeye yönelik bir yakınlık kurma yöntemidir.[9]

Dijital çağda bu motivasyonlar, bilişim sistemlerinin sağladığı anonimlik ve mağdura erişim kolaylığı ile takibi daha da tehlikeli bir boyuta dönüştürmüştür. Fail, fiziksel dünyada göze alamayacağı taciz eylemlerini, sanal dünyanın sunduğu "görünmezlik zırhı" altında çok daha düşük bir maliyet ve riskle gerçekleştirebilmektedir.[10] Siber takip vakalarında faillerin ana motivasyonu genellikle mağduru 7/24 gözetleyerek onda "her an izleniyorum" hissi yaratmak ve bu yolla sosyal çevresinden izole ederek psikolojik bir çöküşe sürüklemektir.[11] Sonuç olarak ısrarlı takip; failin kendi içsel boşluklarını, intikam arzularını veya kontrol dürtülerini mağdurun özgürlüğü pahasına tatmin etmeye çalıştığı, yıkıcı bir şiddet sarmalıdır.[12]

Israrlı takip (stalking), güncel hukuk doktrininde modern bir suç tipi olarak sınıflandırılmakla birlikte, bir davranış örüntüsü olarak kökenlerinin antik dönemlere kadar uzandığı gözlenmektedir. Bu bağlamda, söz konusu davranış örüntülerinin, binlerce yıl öncesinden itibaren tıp ve edebiyat disiplinlerinde yer aldığı görülmüştür. Hippocrates, Galen ve Plutarch gibi düşünürler, bu tür "takıntılı" davranışlara, *tıbbi bir bakış açısıyla* eserlerinde yer vermişlerdir.[13] Edebiyat ala-

---

6 Cihan (n 1) 342; Hamdiye Yılmaz İmret, 'Kadına Karşı Şiddetin Bir Türü Olarak Israrlı Takip Suçu (TCK'nın 123/A Maddesi)' (2024) 11 İstanbul Üniversitesi Hukuk Fakültesi Dergisi 1 8.

7 Canan Sarı, 'Israrlı Takip Suçunun Kadına Yönelik Şiddetin Önlenmesindeki Önemi' (2025) Terazi Hukuk Dergisi 102; Dülger (n 1) 18.

8 Havle (n 4) 233; Dülger (n 1) 18.

9 Bilal Emre Can, 'Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Yaşar Üniversitesi 2023); Havle (n 4) 233.

10 Gündoğdu (n 3) 10; Güneş (n 3) 16.

11 Güneş (n 3); Subhajit Panda, 'Towards a Cyberfeminist Framework for Addressing Gender-Based Violence in Social Media: An Introduction' (2023) <https://doi.org/10.4018/978-1-6684-8893-5.ch008>.

12 Dülger (n 1) 16; Sarı (n 7) 106.

13 Edward H Reynolds ve James V. Kinnier Wilson, 'Obsessive Compulsive Disorder and Psychopathic Behaviour in Babylon' (2012) 83 Journal of Neurology, Neurosurgery & Psychiatry 199.

nında ise Dante Alighieri, Petrarch ve Søren Kierkegaard gibi önemli şahsiyetlerin eserlerinde ve yaşam öykülerinde, ısrarlı takip davranışlarına benzer saplantılı bağlanma izlerine rastlanmıştır.[14] 19. yüzyılda Fransız psikiyatrist Esquirol, "erotomani"[15] kavramını tanımlayarak, eserlerinde bu davranışın klinik temellerini oluşturmuştur.[16] 20. yüzyılın başlarında, bu tür eylemler "sosyal saldırganlık" ve "zorbalık" bağlamında değerlendirilirken, "stalking" terimi ancak yüzyılın sonlarına doğru modern kriminoloji sözlüğüne girmiştir.[17]

*Çağımızda* teknoloji alanında meydana gelen gelişmeler sonucunda bilişim sistemleri ve sosyal medya, günlük yaşamın ayrılmaz bir parçası haline gelmiştir.[18] 2024 yılının sonlarına doğru ve 2025 yılının başlarında, dünya çapında aktif sosyal medya kullanıcılarının sayısının 5 milyarı aştığı bildirilmektedir. Bu veri, dünya nüfusunun yaklaşık %62,3'üne karşılık gelmektedir.[19] Her gün yaklaşık bir milyon yeni kullanıcının sosyal medya dünyasına adım atması, bilişim sistemlerinin toplumun en temel yapı taşlarına ne kadar hızlı bir şekilde entegre olduğunu ortaya koymaktadır.[20] Türkiye'de internet kullanım oranının %88,3'e ulaştığı tespit edilmiştir. 2025 yılı verilerine göre, ülkemizde 58,5 milyon kişi aktif olarak sosyal medya kullanmakta olup, bu sayı Türkiye nüfusunun %66,7'sine karşılık gelmektedir.[21]

Bu durum, bireylerin dijital platformlar üzerinde bıraktığı veri izlerinin hacmini artırırken, söz konusu verilerin kötüye kullanım potansiyelini de içinde barındırmaktadır.[22] Statista'ya göre, dünya genelinde internet kullanıcılarının günlük ortalama sosyal medya kullanım süresi 2012 yılında 90 dakika iken, 2023

---

14 Nesrin Duman, Hürmüs İrem Öçalan ve İlayda Çoban, 'Partner Israrlı Takibi Veya Stalklama: Mağdur ve Saldırgan Karakteristikleri ve Stalklama Taktikleri' (2023) 7 Yaşam Becerileri Psikoloji Dergisi 33 ; Selin Türkoğlu, 'Türk Ceza Hukuku Açısından Israrlı Takip' (Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi 2019).

15 Bir kişinin kendisine âşık olduğuna dair hayali inanç.

16 Brendan D Kelly, 'Love as Delusion, Delusions of Love: Erotomania, Narcissism and Shame' (2018) 44 Medical Humanities 15 (Erişim Tarihi: 3 May 2026).

17 Hatice Demirdağ, 'Sosyal Medya Kullanımı ve Dijital Bir Hastalık Olarak Stalkıng' (Yayımlanmamış Yüksek Lisans Tezi, Bolu Abant İzzet Baysal Üniversitesi 2025) 43.

18 Venugeetha Y, Ranjeet Rathod ve Rishabh Kumar, 'Social Networking Sites in Daily Life: Benefits and Threats' [2022] Artificial Intelligence and Communication Technologies 51.

19 Miraç Fırat Çoğan, 'Türk Hukukunda Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Erzincan Binali Yıldırım Üniversitesi 2024) 33.

20 Hilal Almarabeh ve Amjad Sulieman, 'The Impact Of Cyber Threats On Social Networking Sites' (2019) 10 International Journal of Advanced Research in Computer Science 1.

21 Gülden Demir, 'Ekranın Ötesindeki Gençlik: Dijital Medya Ve Gençlik Söylemlerine Eleştirel Bir Yaklaşım' (2025) 5 Journal of Communication Science Researches 253; Büşra Durmuş ve Damla Eyüboğlu, 'Çocuklarda Ekran ve Sosyal Medya Bağımlılığı' (2025) 47 Osmangazi Tıp Dergisi 65.

22 Özge Şenses ve İlknur Aydoğdu Karaaslan, 'Sosyal Medyada Stalklamak Üzerine Yapılan Bir Araştırma' (2022) 5 Sosyal, Beşerî ve İdari Bilimler Dergisi 1527.

yılında 151 dakikaya yükselmiştir.[23] Bu artış, bireylerin dijital ortamdaki takip edilebilirlik sürelerinin uzamasına yol açmaktadır.[24]

Dijital dünyada "takip edilebilir" (traceable) olmak, bireyin yaşamının neredeyse her anının veri haline gelmesi ciddi hukuki ve kriminolojik riskler barındırmaktadır. Bireylerin dijital ayak izi bırakması, sosyal medya paylaşımları, konum bildirimleri (check-in), etiketlemeler ve çevrimiçi alışkanlıklar vasıtasıyla gerçekleşmektedir.[25] Bu izler sayesinde fail bilişim sistemlerini kullanarak mağdurun günlük alışkanlıklarını, sosyal çevresini ve fiziksel yerini kolayca tespit edebilmektedir.[26]

Dijital platformlar, bireyin özel yaşamı ile kamusal alanı arasındaki sınırı muğlaklaştırmaktadır.[27] Kişisel verilerin korunmasına yönelik farkındalığın düşük olması kullanıcıların "gizlilik" yerine "etkileşim" odaklı hareket etmelerine yol açmaktadır. Failler mağdurları sosyal medya hesabını kapatsalar bile, geçmişte bıraktıkları dijital izler veya ortak arkadaşlar vasıtasıyla dolaylı olarak izleyebilmektedirler.[28]

Dijital dünyada takip edilebilir olmanın yarattığı bir diğer sorun ise failin anonimliğidir.[29] Mağdur dijital izleriyle tamamen "görünür" ve "takip edilebilir" durumdayken, fail sahte hesaplar, VPN veya proxy gibi araçlar arkasına gizlenebilmektedir.[30] Bu durum, mağdurun korku ve çaresizlik duygularını artırırken, adli makamların faili belirlemesini ve dijital kanıtların doğruluğunu sağlamasını zorlaştırmaktadır.[31]

Teknolojinin yaygınlaşması ve siber ortamın anonim yapısının oluşturduğu riskler, dünya genelinde birçok ülkede siber ısrarlı takip eylemlerinin suç haline getirilerek cezai yaptırımlarla caydırıcılıklarının artırılmasına çalışılmıştır.[32]

---

23 'Küresel Günlük Sosyal Medya Kullanımı 2025 | Statista' <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/> (Erişim Tarihi 8 Mayıs 2026).

24 Özge Şenses ve diğerleri, 'Toplumsal Cinsiyet Bağlamında Siber Takip Üzerine Yapılan Bir Araştırma' (2023) 3 Türkiye Medya Akademisi Dergisi 185.

25 Türkoğlu (n 14) 18.

26 ibid.

27 Halil İbrahim Özbilger, 'Sosyal Medyada Kişisel Verilerin Korunmasına İlişkin Bir Araştırma' (2025) 7 Kişisel Verileri Koruma Dergisi 35 <https://dergipark.org.tr/en/pub/kvkd/article/1633255>.

28 Özge Ayas ve Nilüfer Mutlu, 'Siber Ortamda Kadınlara Karşı Gerçekleşen Israrlı Takip Suçunun Eleştirel Analizi' Cinsiyet Bağlamında Hukuka Eleştirel Bakış Sempozyumu (Atılım Üniversitesi, 2024).

29 Şaban Cankat Taşkın, 'Israrlı Takip Suçu' (2023) 10 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 91.

30 Gündoğdu (n 3) 10.

31 Ayas ve Mutlu (n 28) 277.

32 Taşkın (n 29); Gündoğdu (n 3); Ayşenur Çalışkanlar Aşılıoğlu, 'Kadına Yönelik Şiddet Türlerinden Takip: 6284 Sayılı Kanun ve Türk Ceza Kanunu Önleme ve Koruma' (Yayımlanmamış Yüksek Lisans Tezi, Trakya Üniversitesi 2024); Panda (n 11).

Bu çalışmada, bilişim sistemleri aracılığıyla gerçekleştirilen ısrarlı takip suçunu, detaylı bir şekilde incelemeyi amaçlıyoruz. Çalışma kapsamında, öncelikle ısrarlı takip suçunun genel çerçevesi çizilecek, ardından bilişim sistemleri ve iletişim araçlarının bu suçun işlenmesindeki rolü tartışılacaktır. Daha sonra, siber ısrarlı takip suçuyla *mücadelede karşılaşılan zorluklar* değerlendirilecek ve çözüm önerileri sunulacaktır.

## I. KAVRAMSAL VE TEORİK ÇERÇEVE

Israrlı takip suçunun (TCK m. 123/A) hukuki sınırlarını ve koruduğu hukuki değeri tam anlamıyla belirlemek için, öncelikle bu suçun dayandığı kavramsal ve teorik temellerin açıklanması gerekmektedir. *Çünkü bu temeller, suçun hem maddi unsurlarının tanımlanmasında hem de dijitalleşen dünyada ortaya çıkan yeni biçimlerinin hukuki değerlendirilmesinde kritik bir anahtar işlevi görmektedir*.[33] Bu bölümde, ısrarlı takip eyleminin bireyin hareket özgürlüğü ve psikolojik bütünlüğü üzerinde nasıl sistematik bir baskı mekanizması oluşturduğunun açıklanması hedeflenmektedir.

Bu kapsamda, ilk olarak "ısrarlı takip" kavramının mahiyeti ve tarihsel gelişimi ele alınacak, daha sonra suçun maddi dünyadaki izdüşümü olan "fiziki takip" ile dijital dünyadaki karşılığı olan "siber takip" arasındaki kavramsal köprüler kurulacaktır. Sonrasında, suçun tipiklik unsurlarının ortaya çıkması bağlamında, ısrarlı takibin kişilerin huzur ve sükununu bozma (TCK m. 123), tehdit (TCK m. 106), cinsel taciz (TCK m. 105) ve özel hayatın gizliliğini ihlal (TCK m. 134) gibi benzer suç türlerinden hangi karakteristik özelliklerle ayrıldığı ve mobbing ile siber zorbalık gibi modern şiddet türleriyle olan ilişkisi ele alınacaktır. Son bölümde, siber takip ile yine bilişim sistemleri vasıtasıyla işlenen siber taciz, doxxing, izinsiz ifşa (intikam pornografisi) ve deepfake taciz gibi eylem türleri arasındaki ilişkiler incelenerek, siber takibin teorik sınırları güncel doktrinel tartışmalar çerçevesinde belirlenecektir. Bu teorik zemin, çalışmanın ilerleyen bölümlerinde ele alınacak olan uygulamadaki teknolojik sorunların ve reform önerilerinin hukuki tutarlılığını sağlamak açısından hayati bir önem taşımaktadır.

### A. Israrlı Takip Kavramı

Israrlı takip İngilizcede "stalking" kelimesinden gelmekte olup, eski İngilizcede avcılık bağlamında kullanılan, "sinsice yaklaşmak", "gizlice takip etmek" veya "yavaş ve sessiz adımlarla izlemek" fiillerine karşılık gelen "stalk"tan türemiştir.[34] Türk hukuk terminolojisinde ise bu kavramın karşılığı 'musallat olma', 'dadanma' veya 'sırnaşma' gibi eylemlerdir.[35] Başlangıçta avcılık terimi olarak kullanılan stalking kelimesi (avına gizlice yaklaşma), 1990'lı yıllarda ünlülerin

[33] Dülger (n 1) 36.

[34] Yılmaz İmret (n 6) 9.

[35] ibid.

saplantılı hayranları tarafından takip edilmesiyle hukuki bir anlam kazanmıştır.[36] Bu tür davranışlar, bireylerde korku ve kaygı yaratan, istenmeyen ve sürekli psikolojik ve fiziksel şiddet içeren bir bütün olarak değerlendirilmektedir.[37]

Israrlı takip kavramı uzun yıllardır bilinen bir olgu olmasına rağmen, hukuki terminolojideki anlamını yakın bir dönemde kazanmıştır.[38] Hukuki anlamda ısrarlı takip, tek bir eylemden ziyade bir "davranışlar örüntüsü" olarak tanımlanır.[39] Söz konusu örüntü, mağdurun rızasına aykırı şekilde tekrar eden, tehdit, taciz, cinsel taciz, gözetim veya istenmeyen iletişim içeren eylemleri kapsamaktadır.[40] Bu tür eylemlerin ortak özelliği, mağdur üzerinde korku, endişe veya huzursuzluk yaratma potansiyeli taşıması ve tekrar etmesi nedeniyle mağdurun yaşam kalitesini olumsuz olarak etkilemesidir.[41]

Türk Ceza Kanunu'nda bu kavram 'ısrarlı takip' olarak adlandırılmış ve madde metninde, bu eylemlerin mağdurda ciddi bir rahatsızlık veya güvenlik kaygısı yaratması durumunda suçun oluşacağı açıkça belirtilmiştir.[42]

### B. Israrlı Takip Kavramının Benzer Kavramlardan Farkı

Türk Ceza Kanunu'nun 123/A maddesiyle düzenlenen ısrarlı takip suçu, korunan hukuki değer ve suçun unsurları açısından kanundaki bazı suç tipleriyle benzerlik taşısa da, kendine özgü yapısı ve içerdiği ısrar unsuru ile bu suçlardan ayrılmaktadır.[43] Bu suçun diğerlerinden temel farkı, belirli bir eylemden ziyade, bir dizi tekrarlayan davranışın birleşerek mağdurda korku, endişe veya huzursuzluk hissi ortaya çıkarmasıdır.[44] Özellikle 6284 sayılı Ailenin Korunması ve Kadına Karşı Şiddetin Önlenmesine Dair Kanun'da "tek taraflı ısrarlı takip" olarak tanımlanan bu durum, failin, mağdurda ciddi bir huzursuzluk oluşturacak veya kendisinin veya aralarında aile bağı olsun veya olmasın yakınlarının güvenliğin-

---

36 Sarı (n 7) 107.

37 Demet Başar ve Nuray Sakallı Uğurlu, 'Israrlı Takip: Tanımı ve Sosyal Psikolojik Değişkenler ile İlişkileri' (2021) 24 Türk Psikoloji Yazıları 22.

38 "Stalking" terimi, modern hukuk terminolojisine ilk olarak 1990 yılında Amerika Birleşik Devletleri'nin Kaliforniya eyaletinde müstakil bir suç tipi olarak girmiş ve bu tarihten itibaren küresel düzeyde yasallaşma sürecine başlamıştır. Özellikle İstanbul Sözleşmesi›nin 34. maddesiyle getirilen «başka bir kişiye yönelik gerçekleştirilen ve bu kişinin güvenliğinden korkmasına neden olan kasıtlı bir davranışlar örüntüsünü suç haline getirme» yükümlülüğü, kavramın uluslararası hukukta standart bir tanıma kavuşmasında ve üye ülkelerin iç hukuk düzenlemelerinde ortak bir alt yapı oluşturulmasında dönüm noktası olmuştur.

39 Duman, Öçalan ve Çoban (n 14) 4.

40 Sarı (n 7) 108.

41 ibid.

42 Yusuf Gürleyen, 'Türk Ceza Kanunu'nda Israrlı Takip Suçu (TCK m. 123/A)' (Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2024) 9.

43 Havle (n 4) 235.

44 Dülger (n 1) 25.

den endişe duymasına neden olabilecek her türlü fiziki takip veya haberleşme ve iletişim araçlarını, bilişim sistemlerini veya üçüncü kişileri kullanarak temas kurmaya çalışma eylemlerini kapsamaktadır.[45]

### 1. TCK m. 123 Kişilerin Huzur ve Sükununu Bozma Suçu

Israrlı takip suçu TCK m. 123'te tanzim edilen kişilerin huzur ve sükununu bozma suçundan farklılık arz etmektedir. Israrlı takip suçu oluşturulmadan önce, bu tür davranışlar TCK m. 123 çerçevesinde ele alınmaktaydı.[46] Bununla birlikte, TCK m. 123/A'nın, TCK m. 123'e kıyasla özel bir norm olarak kabul edildiği düşünülmektedir.[47] Bu iki suç arasındaki ilk fark ısrar unsurunun niteliğidir. TCK m. 123'te ısrar, suçun tek bir defa işlenmesiyle de oluşabilirken, ısrarlı takipte eylemlerin tekrarlayıcı ve süreklilik arz eden bir örüntü oluşturması zorunludur.[48] İki suç arasındaki bir diğer fark ise netice itibarıyla meydana gelen etkinin niteliğidir; zira TCK m. 123 kişilerin huzur ve sükununu bozmayı hedeflerken, TCK m. 123/A doğrudan mağdurun kendisini güvende hissetme hakkına yönelik daha ağır bir ihlali cezalandırmaktadır.[49] TCK m. 123'te düzenlenen suçun oluşumu için sadece huzur ve sükunun bozulması yeterlidir. Buna karşılık, ısrarlı takip suçunda ise mağdurun kendisinin veya yakınlarının güvenliğinden ciddi bir korku duyması, çaresizlik hissetmesi veya yaşam biçimini değiştirmek zorunda kalması gibi daha ağır ve spesifik neticelerden en az birinin gerçekleşmesi aranır.[50]

---

45 Betül Çelebi Dağ, 'Israrlı Takip İle Yetişkin Ebeveyn Kabul-Ret Algısı Arasındaki İlişkide Kişilik Bozukluklarının Aracı Rolü' (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Gedik Üniversitesi 2022) 14.

46 Yargıtay'ın 07.04.2025 tarih ve 2022/911 E., 2023/145 K. Kararına konu olayda sanık, eski birlikte yaşadığı müştekinin evine giderek, aracının camlarına vurarak ve uzaklaştırma kararına rağmen onu rahatsız ederek taciz etmiştir. Yerel mahkeme (İzmir 19. Asliye Ceza Mahkemesi), sanığı 2022 yılında Türk Ceza Kanunu'na yeni eklenen "Israrlı Takip" (TCK 123/A) suçundan cezalandırmıştır. Ancak sanığın bu eylemleri gerçekleştirdiği tarihler Aralık 2021 ve Ocak 2022'dir. "Israrlı Takip" suçu Türk Ceza Kanunu'na Mayıs 2022'de eklenmiştir. Yani sanık eylemi gerçekleştirdiğinde, hukuk sistemimizde henüz "Israrlı Takip" diye müstakil bir suç tipi bulunmamaktaydı. Bundan dolayı Yargıtay, Adalet Bakanlığı'nın "kanun yararına bozma" istemini haklı bularak kararı zaman bakımından uygulama hatasından dolayı bozmuştur Yargıtay kararında "TCK'nın 7/1. maddesi uyarınca, bir kimse işlendiği zaman kanunda suç sayılmayan bir fiilden dolayı cezalandırılamaz. Sanığın eylemleri "Israrlı Takip" suçundan değil, o tarihte yürürlükte olan "Kişilerin Huzur ve Sükununu Bozma" (TCK 123) suçu kapsamında değerlendirilmelidir" şeklinde belirtmiştir. Yargıtay'ın benzer nitelikteki kararları için bakınız. 12. CD., E. 2024/167 K. 2024/4106 T. 11.9.2024; 12. CD., E. 2023/5745 K. 2025/181 T. 7.1.2025.

47 Taşkın (n 29) 96; Aybike Berber Yörük, 'Mevzuatımızda Yeni Bir Suç Tipi: "Israrlı Takip"' (2025) 11 İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 169.

48 Ertuğrul Ünal, 'Israrlı Takip Suçunda Yer Alan Israr Kavramının Hukuki Niteliği ve Suç İçin Öngörülen Yaptırım Özelinde Tehdit Suçuyla İlişkisi Üzerine Bir Değerlendirme' (2024) 9 İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi 549.

49 Cihan (n 1) 343.

50 Taşkın (n 29) 175. Yargıtay'ın tehdit ve ısrarlı takip suçu içeren kararları için bakınız. 9. CD., E. 2025/1274 K. 2025/6567 T. 15.9.2025; 23. CD., E. 2015/15811 K. 2016/7603 T. 13.6.2016; 6. CD., E. 2024/2435 K. 2024/8411 T. 2.7.2024; 6. CD., E. 2024/2371 K. 2024/7344 T. 10.6.2024.

**2. TCK m. 106 Tehdit Suçu**

Israrlı takip suçu, TCK m. 106'da düzenlenen tehdit suçundan da ayrılmaktadır. Tehdit suçunda gelecekte bir kötülüğün yapılacağına ilişkin beyan esas teşkil ederken, ısrarlı takipte bu tür bir beyan olmaksızın dahi mağdurda ciddi bir güvenlik endişesinin oluşmasına yol açabilen bir davranış örüntüsü mevcuttur.

Israrlı takip eylemleri genellikle örtülü bir tehdit unsuru içerse de, bu iki suç türü yapısal olarak farklılık göstermektedir.[51]İlk farklılık, suç tiplerinin kapsamına ilişkindir. Tehdit suçunun temelini mağdurun gelecekte bir kötülüğe maruz kalacağına dair bir beyan teşkil etmektedir. Israrlı takip suçunda ise, failin mutlaka bir kötülük yapacağına ilişkin beyanda bulunma zorunluluğu mevcut değildir. Fiziksel takip veya bilişim sistemleri üzerinden kesintisiz iletişim kurma gayretiyle mağdur üzerinde bir baskı oluşturulması söz konusudur.[52] İkinci farklılık, suç tiplerinin fiil yapılarındaki ayrım noktasında ortaya çıkmaktadır: Tehdit suçunun oluşumu ani bir fiilin icrasını gerektirmekte iken, ısrarlı takip suçunun varlığı tipik olarak bir süreci (davranış örüntüsünü) gerektirmektedir.[53] Eğer fail, mağduru takip ederken aynı zamanda tehdit ediyorsa, genel olarak TCK m. 123/A hükmü uygulanacaktır. Ancak, tehdit eylemi bağımsız ve belirgin bir ağırlık taşıyorsa, içtima müessesesi dikkate alınmalıdır.[54]

**3. TCK m. 105 Cinsel Taciz Suçu**

Israrlı takip suçu, cinsel taciz suçundan da farklıdır. Cinsel taciz suçu, mağdurun cinsel dokunulmazlığını ihlal eden davranışları kapsarken, ısrarlı takip suçunun temelinde mağdurun huzur ve güvenliğinin bozulması yatar.[55] Cinsel taciz suçunun oluşumu için failin cinsel bir saik ile hareket etmesi zorunludur.[56] Ancak, ısrarlı takip suçunda failin motivasyonunun önemli olmadığı kabul edilmektedir; çünkü failin öfke, intikam, saplantılı sevgi veya kontrol isteği gibi farklı nedenlerle hareket etmesi mümkündür.[57] İki suç türü arasındaki bir başka temel fark, işlenme şekillerinde ortaya çıkmaktadır. Cinsel taciz genellikle anlık bir eylem olabilmesine karşın, ısrarlı takip suçu niteliği gereği bir süreklilik ve tekerrür eden davranışlar bütünüdür.[58] Fail, mağdura cinsel içerikli olmayan mesajlar

---

51 Balcı ve Çakır (n 2) 325.

52 Ünal (n 48) 554; Dülger (n 1) 32.

53 Ünal (n 48) 555.

54 Muhammed Emre Tulay, 'Israrlı Takip Suçunun Suç Teorisi İle Uyumu Üzerine Bir Değerlendirme' (2024) 14 Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi 57; Ayşe Tuğçe Boz Çelik, 'Türk Ceza Hukukunda Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi 2025) 23.

55 Balcı ve Çakır (n 2) 326.

56 Çağlasın Yaldız, 'Yargıtay Kararları Işığında Cinsel Taciz Suçu ve İncelemesi' (2023) 7 The Journal of Social Science 213.

57 Duman, Öçalan ve Çoban (n 14) 4; Başar ve Uğurlu (n 41) 27.

58 Buket M Soygüt, 'Kadına Yönelik Erkek Şiddetinin Önlenmesi Bağlamında Stalking (Israrlı Takip) ve Cezasızlık Sorunu' (2020) 5 Çankaya Üniversitesi Hukuk Fakültesi Dergisi 2781.

gönderdiğinde veya yalnızca uzaktan izleme (stalking) yoluyla ısrarlı bir şekilde takip ettiğinde, bu durum ısrarlı takip suçunu oluşturur; ancak mesajların içeriği cinsel bir boyut kazandığında, bu eylem cinsel taciz suçuna dönüşmektedir.[59]

### 4. TCK m. 134 Özel Hayatın Gizliliğini İhlal Suçu

Israrlı takip suçu ile özel hayatın gizliliğini ihlal suçu arasında önemli farklılıklar bulunmaktadır. Bu iki suç tipini ayıran temel farklılık, suçları oluşturan fiillerin odak noktalarında belirginleşmektedir. Türk Ceza Kanunu'nun 134. maddesi bireyin mahremiyet alanına yönelik müdahale teşkil eden fiilleri (örneğin, izinsiz fotoğraf alma veya ses dinleme eylemleri) müeyyide altına alınmaktadır.[60] Israrlı takip suçunda ise, failin mağdurun mahrem alanına fiziki bir müdahalede bulunmaksızın dahi (örneğin, umumi bir alanda takibi yahut dijital iletişim mecraları aracılığıyla kesintisiz ileti gönderimi vasıtasıyla) mağdur üzerinde bir baskı unsuru oluşturması söz konusudur.[61] İki suç türü arasındaki bir başka fark, temas kurma eyleminin doğasında ortaya çıkmaktadır. Israrlı takip fiilinde failin motivasyonu çoğunlukla mağdurla bir temas tesis etme (fiziksel yahut dijital yollarla) gayesini taşırken[62], özel hayatın gizliliğini ihlal suçunda ise esas amaç, genellikle gizlilik arz eden bilgi veya görsellerin elde edilmesidir.[63]

### 5. İşyerinde Psikolojik Taciz (Mobbing)

Israrlı takip suçu iş yerinde psikolojik tacizden (mobbing) farklıdır. Mobbing ile ısrarlı takip arasındaki en temel fark, mekânsal bağlam ve failin amacı üzerinde yoğunlaşmaktadır. Mobbing, iş dünyasında ortaya çıkan ve bir çalışanın iş yerinden uzaklaştırılması ya da yıldırılması amacıyla gerçekleştirilen sistematik bir psikolojik baskı türünü ifade eder.[64] Oysa ısrarlı takip suçunda mağdur ile fail arasında bir iş ilişkisi olması gerekmezken, failin amacı genellikle mağdurun işten çıkarılmasını sağlamak değil, aksine, mağdur üzerinde tam bir kontrol kurmak ya da saplantılı bir ilişki geliştirmektir.[65] Ancak, Türk Ceza Kanunu'n-

---

59 Ayas ve Mutlu (n 28) 277; Taşkın (n 29) 98; Yargıtay'ın ısrarlı takip ve cinsel taciz suçlarını içeren kararları için bakınız. 1. CD., E. 2012/5963 K. 2013/3240 T. 17.04.2013; 14. CD., E. 2019/7006 K. 2019/13675 T. 26.12.2019; 6. CD., E. 2023/18458 K. 2024/2999 T. 5.3.2024; 1. B., B. 2014/2302 T. 9.11.2017.

60 Mustafa Alıcı, 'Özel Hayatından Dolayı Memura Disiplin Cezası Verilebilir Mi?' (2019) 5 Gümrük ve Ticaret Dergisi 44.

61 Dülger (n 1) 35; Başar ve Uğurlu (n 41) 28.

62 Gündoğdu (n 3) 8.

63 Can (n 9) 15; Yargıtay'ın ısrarlı takip ve özel hayatın gizliliğini ihlal suçları kararları için bakınız. 9. CD., E. 2023/10 K. 2023/1975 T. 4.4.2023; 6. CD., E. 2023/16555 K. 2024/596 T. 16.1.2024; CGK., E. 2023/355 K. 2023/492 T. 4.10.2023.

64 Hasan Yılmaz ve Abubekir Kaymaz, 'Kurumsal Bir Risk Unsuru: Mobbing (İş Yerinde Psikolojik Taciz)' [2016] Denetişim 73; Banu Özden, 'Türk İş Hukuku Kapsamında Psikolojik Taciz (Mobbing)' (2018) 5 Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi 22.

65 Duman, Öçalan ve Çoban (n 14) 4.

da mobbing eylemi bağımsız bir suç olarak sınıflandırılmamışken, ısrarlı takip eylemi, TCK'nın 123/A maddesi çerçevesinde ayrı bir suç olarak yasal düzenlemeye tabi tutulmuştur.[66]

**6. Zorbalık**

Israrlı takip, zorbalıktan farklıdır. Zorbalık, genellikle bir kişinin fiziksel veya sosyal güç üstünlüğünü kullanarak başka bir kişiyi aşağılaması ya da üzerinde baskı kurması şeklinde tanımlanır. Bu tür eylemler genellikle eğitim ortamında ve akran grupları arasında fiziksel şiddet unsurlarıyla meydana gelmektedir.[67] Siber zorbalık, bilişim teknolojileri aracılığıyla itibar zedeleme veya psikolojik zarar verme amacı güden, modern şiddet olgusunun daha geniş bir biçimi olarak tanımlanır.[68] Israrlı takip eylemi, siber zorbalığın aksine, sadece dijital ortamla sınırlı kalmayıp, failin mağdurla 'iletişim kurma çabası' üzerine kuruludur.[69] Gerçekten de, zorbalık eylemlerinde mağdurun aşağılanması ana unsurken, ısrarlı takipte mağdurun yaşamının sürekli izlenmesi ve rızası dışında temas kurulması temel bir motivasyon olarak öne çıkmaktadır.[70]

**7. İstenmeyen Elektronik İleti Gönderme (Spam)**

Israrlı takip, spam olarak bilinen istenmeyen elektronik ileti göndermeden farklı bir hukuki özellik taşımaktadır. İstenmeyen elektronik ileti" (spam), genellikle ticari amaçlarla ve reklam içerikli olarak gönderilen mesajları kapsamaktadır.[71] Israrlı takip suçu (TCK m. 123/A), kasıtlı ve sürekli davranışlarla oluşmaktadır.[72] Ancak istenmeyen elektronik ileti göndermeden farklı olarak, ısrarlı takipte fail, mağdurun kimliğini hedef alarak ona ciddi bir huzursuzluk veya güvenlik kaygısı yaşatmaktadır.[73] Israrlı takip, spam eyleminden temas kurma biçimi yönünden de farklılaşmaktadır. Sosyal medya platformları üzerinden sürekli olarak "arkadaşlık isteği" gönderilmesi ya da mağdurun rızası dışında kişisel mesajlar yoluyla iletişimin sürdürülmesi, ısrarlı takip fiili kapsamına girmektedir. Ancak, genel nitelikteki ticari reklam mesajları, bu suçun "temas kurma" unsurunu taşımadığı

---

66 Süleyman Özar, 'Israrlı Takip Suçu (TCK m. 123/A) 2' (2022) 71 Ankara Üniversitesi Hukuk Fakültesi Dergisi 1397.

67 Can (n 9) 16; Mobbing ile ilgili Yargıtay kararları için bakınız. 9. HD., E. 2014/2273 K. 2014/14184 T. 5.5.2014; 22. HD., E. 2013/693 K. 2013/30811 T. 27.12.2013; 22. HD., E. 2014/2157 K. 2014/3434 T. 21.2.2014; HGK., E. 2014/110 K. 2015/2600 T. 11.11.2015.

68 Ayas ve Mutlu (n 28) 278.

69 Taşkın (n 29) 98.

70 Ayas ve Mutlu (n 28) 278; Zorbalık ile ilgili Yargıtay kararları için bakınız. 4. CD., E. 2012/25142 K. 2014/1335 T. 21.1.2014; 6. CD., E. 2014/15547 K. 2015/965 T. 3.2.2015; 18. CD., E. 2015/6408 K. 2015/13937 T. 21.12.2015; 4. HD., E. 2014/16557 K. 2015/1240 T. 2.2.2015.

71 Ünal Öztürk, 'Sanal Ortamda Haksız Rekabet Hâlleri' (2021) 1 Konya Barosu Dergisi 71.

72 Dülger (n 1) 35.

73 Ayas ve Mutlu (n 28) 279.

için değerlendirme dışı bırakılmaktadır; çünkü bu tür iletilerde bireyin kişiliğine yönelik takıntılı bir izleme modeli bulunmamaktadır.[74]

### C. Bilişim Sistemleri Vasıtasıyla İşlenen Israrlı Takip ve İlişkili Kavramlar

Dijitalleşme, geleneksel suç türlerini siber dünyaya taşırken, eylemin gerçekleştirilme biçimi, kullanılan teknoloji ve ihlal edilen hukuki değer doğrultusunda yeni alt kavramların oluşmasına olanak tanımıştır.[75] Bu kavramların her biri, bilişim sistemlerini bir araç olarak kullanırken, farklı saldırı kalıplarını temsil etmektedir. Özellikle ısrarlı takibin bilişim sistemleri aracılığıyla gerçekleştirilmesi siber zorbalık[76], siber taciz ve siber takip gibi terimlerle örtüştüğü düşünülmekle birlikte; bu kavramlar arasında hukuki nitelik ve uygulama açısından belirgin farklılıklar bulunmaktadır.[77]

#### 1. Bilişim Sistemleri Vasıtasıyla Israrlı Takip

Bilişim sistemleri vasıtasıyla ısrarlı takip, bilişim sistemlerinin (sosyal medya, e-posta, GPS, casus yazılımlar) bir kişi tarafından başka bir kişinin rızası dışında sistematik olarak izlenmesi ve onunla temas kurulmaya çalışılması olarak kabul edilmektedir.[78] Bu durum, failin mağdura fiziksel olarak yaklaşmadan da baskı uygulayabilmesine olanak tanımaktadır.[79] Buna göre e-posta, WhatsApp, Skype gibi platformların hem iletişim aracı hem de bilişim sistemi olarak değerlendirilebileceği dikkate alındığında, bu platformlar üzerinden ısrarlı biçimde mesaj gönderilmesiyle mağdurun huzur ve sükûnunun bozulması, ısrarlı takip suçunu teşkil etmektedir.[80] Bu suçun işleniş şeklinde fail, mağdurun dijital ayak izlerinin takibini, sürekli mesaj iletimini, sahte hesaplar üzerinden denetimi yahut mağdurun konumunun dijital araçlarla izlenmesini kapsayan eylemlerde bulunmaktadır.[81] Bilişim sistemleri aracılığıyla yapılan ısrarlı takip, benzer eylemlerden farklı olarak, mağdurla sürekli bir "iletişim kanalı" açık tutmayı ve ona her an izleniyormuş gibi hissettirerek psikolojik baskı kurmayı amaçlamaktadır.[82]

---

74 Çalışkanlar Aşılıoğlu (n 34) 18; Spam ile ilgili Yargıtay kararları için bakınız. 23. HD., E. 2014/546 K. 2014/4652 T. 17.06.2014; HGK., E. 2012/550 K. 2012/820 T. 21.11.2011; 4. HD., E. 2022/14023 K. 2024/13344 T. 19.12.2024; 11. HD., E. 2021/3731 K. 2022/9004 T. 13.12.2022.

75 Buket Cansu Uludağ ve Serdal Fidan, 'Rutin Aktiviteler Teorisi Bağlamında Dijitalleşen Dünyada Siber Suç Mağdurları' (2023) 4 Habitus Toplumbilim Dergisi 175.

76 Mihriban Hekim, 'Ceza Hukuku Açısından Siber Zorbalık' (2024) (Erişim Tarihi: 4 May 2026).

77 Ayas ve Mutlu (n 28) 278; Çoğan (n 17) 33.

78 Gündoğdu (n 3) 9.

79 Şule Karataş, 'Türk ve Alman Hukukunda Israrlı Takip Suçunun Ceza Genel Teorisi Açısından İncelenmesi' (2026) 16 Hacettepe Hukuk Fakültesi Dergisi 769.

80 Balcı ve Çakır (n 2) 326.

81 Taşkın (n 29) 99; Siber takip ile ilgili Yargıtay kararları için bakınız. 3. CD., E. 2021/9141 K. 2022/5934 T. 11.10.2022; 3. CD., E. 2021/12426 K. 2022/6939 T. 20.10.2022; 3. CD., E. 2021/13215 K. 2023/7582 T. 19.10.2023; 3. CD., E. 2022/11685 K. 2024/3488 T. 7.3.2024.

82 ibid.

**2. Siber Taciz**

Siber taciz, genellikle siber ısrarlı takibi de ihtiva eden daha geniş bir üst bir kategori olarak kabul edilir.[83] Siber taciz, çevrimiçi platformlarda rahatsız edici, tehditkâr veya düşmanca davranışları içerirken; ısrarlı takip, mağdurla sürekli iletişim kurarak onu huzursuz etme eylemlerine özellikle dikkat çeker. Siber taciz, genellikle tek seferlik bir eylemle de gerçekleşebilirken, siber ısrarlı takipte eylemlerin tekrarlayıcı ve süreklilik arz etmesi temel bir farklılaştırıcı nitelik oluşturmaktadır.[84]

Bu bağlamda siber takip, siber zorbalığın değil, siber tacizin bir türü olarak değerlendirilmelidir.[85] Siber tacizin işleniş şekli mağduru rahatsız edici, küçük düşürücü veya tehditkâr içerikli iletilerin tek seferlik veya kümülatif olarak gönderilmesini kapsar. Israrlı takipte 'izleme ve denetleme' unsuru ön planda tutulurken, siber tacizin odak noktası mağdurun huzur ve sükûnunu ihlal edici nitelikteki saldırgan içerikli mesajların bulunmasıdır.[86]

---

83 ibid.

84 Esra Solmaz Yiğit, 'Ergenlerin Bağlanma Stilleri İle Psikolojik İhtiyaçları Arasındaki İlişkide Israrlı Takip Edilmenin Aracılık Rolü' (Yayımlanmamış Yüksek Lisans Tezi, Karamanoğlu Mehmetbey Üniversitesi 2024) 24; Yargıtay, siber taciz eylemlerini TCK m. 123/A maddesi yürürlüğe girmeden önce ağırlıklı olarak "Kişilerin Huzur ve Sükununu Bozma" veya içeriğinde cinsel motifler barındırması durumunda "Cinsel Taciz" suçları kapsamında değerlendirmekteydi. Yargıtay'ın yerleşik içtihatlarına göre; sosyal medya platformları üzerinden mağdura rızası dışında sistematik mesajlar gönderilmesi, sahte hesaplar açılarak dijital ortamda sürekli izlenmesi veya iletişim bilgilerinin rıza dışı paylaşılması gibi eylemler, mağdurun "ruhsal sükununu bozma kastı" taşıdığı sürece suçun maddi unsurunu oluşturmaktadır. Özellikle 12. Ceza Dairesi'nin kararlarında, siber tacizin cezalandırılabilmesi için eylemlerin belirli bir "yoğunluğa" ulaşması, süreklilik arz etmesi ve mağdurun huzurunu objektif olarak bozacak nitelikte olması gerektiği vurgulanmaktadır. Güncel kararlarda ise bilişim sistemleri vasıtasıyla gerçekleştirilen ve mağdurda ciddi bir korku ya da kaygı uyandıran bu tür siber zorbalık ve taciz faaliyetleri, artık müstakil bir suç tipi olan TCK m. 123/A bağlamında "ısrarlı bir davranış örüntüsü" olarak kabul edilerek yaptırıma tabi tutulmaktadır.

85 Taşkın (n 29) 101; Yargıtay'ın siber taciz kararları için bakınız. Yargıtay 12. Ceza Dairesi, 11.09.2024 tarihli, 2024/167 E., 2024/4106 K.: Farklı numaralardan sürekli arama ve mesaj atma yoluyla mağdurun psikolojik baskı altına alınmaya çalışıldığı vakada; TCK m. 123/A'nın yürürlükte olmadığı bir tarih için ısrarlı takipten hüküm kurulmasını usulden bozsa da mahkemelerin bu tür eylemleri ısrarlı takip olarak nitelendirme iradesini ortaya koymaktadır. Yargıtay 12. Ceza Dairesi, 25.12.2023 tarihli, 2023/874 E., 2023/5864 K.: Bilişim sistemleri aracılığıyla gerçekleştirilen takip ve taciz eylemlerinin hukuki değerlendirmesini içerir. Yargıtay Ceza Genel Kurulu, 13.02.2018 tarihli, 2014/4-821 E., 2018/45 K.: "Israr" kriterinin oluşması için gerekli olan yoğunluk, süreklilik ve eylemler arasındaki zaman aralığının tespiti konusunda emsal teşkil eden karardır. Yargıtay 4. Ceza Dairesi, 09.05.2016 tarihli, 2016/4715 E., 2016/9234 K.: Mağdurun telefon veya sosyal medya yoluyla rahatsız edilmesi eylemlerinde "ısrar" ve "sırf rahatsız etme kastı" unsurlarını değerlendirmiştir. Yargıtay, 23.11.2016 tarihli, 2015/37827 E., 2016/18068 K.: Dijital araçlarla yapılan temaslarda suçun maddi ve manevi unsurlarının belirlenmesine dair bir karardır. Yargıtay 18. Ceza Dairesi, 09.11.2021 tarihli, 2021/2474 E., 2021/7814 K.: Sosyal medya üzerinden gerçekleştirilen taciz eylemlerinin ispatı ve hukuki nitelemesi üzerinedir. Yargıtay 14. Ceza Dairesi, 28.01.2014 tarihli, 2012/8472 E., 2014/1008 K.: İnternet ve bilişim araçları kullanılarak yapılan cinsel içerikli taciz eylemlerine dair bir karardır.

86 Bahtiyar Münir Paltacı, 'Dijital Dünya'nın Tehditleri: Siber Zorbalık Ve Siber İstismar' (2024) 4 Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi 56; Solmaz Yiğit (n 84) 26.

### 3. Kişisel Bilgilerin İfşası (Doxxing)

Kişisel bilgilerin ifşası (doxxing), bir kişinin gerçek kimliğini, ev adresini, telefon numarasını veya diğer kişisel verilerinin, veri sahibinin rızası olmaksızın internet ortamında, genellikle hedef gösterme amacıyla paylaşılması eylemidir.[87] Bu davranış, siber takip eylemleriyle birleştiğinde mağdurun fiziksel güvenliğini dahi tehlikeye atabilecek ciddi sonuçlar doğurma potansiyeline sahiptir ve siber taciz kapsamındaki tehdit edici davranışların tamamlayıcı bir unsuru olarak ortaya çıkabilir.[88] Siber takipte failin asıl amacı mağdurun kamuoyuna ifşası değil, kişisel bilgilerini kullanarak onu izleme ve rahatsız etme eylemlerini gerçekleştirmek ve böylece mağdur üzerinde bir kontrol mekanizması oluşturmaktır.[89] Dolayısıyla, kişisel bilgilerin ifşasının (doxxing) siber zorbalık ve siber takibin bağımsız bir alt türü olmaktan ziyade, bu eylemlerin bir sonucu olarak mağdurun mahremiyetini ihlal eden ve genellikle ikincil bir zarar doğuran bir eylem olarak konumlandırılması gerektiği kanaatindeyiz.

Siber takip ise, mağdurun rızası hilafına gerçekleştirilen sürekli çevrimiçi izleme eylemlerini, sahte profiller vasıtasıyla temasa geçme teşebbüslerini veya dijital mecralarda mağdur hakkında saldırgan içerikli yorumlar yapılmasını ihtiva edebilir.[90] Doxxing eyleminin işleniş şekli incelendiğinde, failin mağdurun özel bilgilerini muhtelif yöntemlerle edinerek bu bilgilerin kamusal platformlarda teşhir edilmesi suretiyle gerçekleştiği görülmektedir.[91] Israrlı takipte fail mağdura

---

87 Paltacı (n 86) 59.

88 ibid.

89 Hivam Özkaya, 'Israrlı Takip Suçunun Düzenlenmesine İlişkin Kademeli Gelişim' (2023) 97 İstanbul Barosu Dergisi 149.

90 Feyzanur Ceylan Özden, 'Kadın Üniversite Öğrencilerinde Siber Obsesif Takip İle Travma Stres Bozukluğu ve Suç Korkusu Arasındaki İlişki' (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa 2025).

91 Paltacı (n 86) 60; Yargıtay içtihatlarında "Doxxing" olarak adlandırılan kişisel bilgilerin rıza dışı ifşası eylemlerini, ağırlıklı olarak TCK m. 136 ("Verileri hukuka aykırı olarak verme veya ele geçirme") ve eylemin içeriğine göre TCK m. 134 ("Özel hayatın gizliliğini ihlal") hükümleri çerçevesinde cezalandırılmaktadır. Yargıtay'ın bu konudaki en temel yerleşik görüşü, bir kişisel verinin (telefon numarası, adres, fotoğraf veya kimlik bilgileri) daha önceden kamuya açık bir alanda bulunmasının, bu verinin üçüncü kişiler tarafından her ne suretle olursa olsun rıza dışı yayılmasına hukuki meşruiyet kazandırmayacağı yönündedir. Kararlarda, mağdurun iletişim bilgilerinin internet sitelerinde veya sosyal medya platformlarında "ısrarlı bir şekilde" ve mağduru huzursuz edecek bir saikle paylaşılması, sadece veri ihlali olarak değil; aynı zamanda eylemin sürekliliğine göre cinsel taciz veya kişilerin huzur ve sükûnunu bozma suçlarıyla (güncel düzenlemede TCK m. 123/A Israrlı Takip) bağlantılı olarak değerlendirilmektedir. Özellikle siber zorbalık ve siber takibin bir aracı olarak kullanılan doxxing eylemleri, mağdurun dijital dünyadaki güvenliğini ve özel hayatının gizliliğini sistemli bir şekilde ihlal eden «zincirleme bir saldırı» olarak kabul edilerek ağır yaptırımlara tabi tutulmaktadır. Bu konudaki Yargıtay kararları için bakınız. 4. CD., E. 2021/26919 K. 2022/13965 T. 2.6.2022; 12. CD., E. 2015/4349 K. 2016/5349 T. 30.3.2016; 12. CD., E. 2015/13758 K. 2017/2514 T. 29.3.2017.

ulaşmaya çalışırken, doxxing eyleminde fail üçüncü kişilerin mağdura ulaşmasını veya ona zarar vermesini sağlayacak bir ortam hazırlamaktadır.[92]

**4. İntikam Pornosu / Rıza Dışı İfşa (Revenge Porn)**

İntikam pornosu / rıza dışı ifşa (revenge porn) normatif düzlemde "cinsel içerikli görüntülerin rıza dışı ifşası" olarak nitelendirilmektedir. Bu davranış, genellikle eski partnerler tarafından intikam veya aşağılama amacıyla, kişilerin özel nitelikli verisi olan görüntülerinin internette ifşa edilmesi şeklinde ortaya çıkmaktadır. Bu tür eylemler, mağdurlar üzerinde derin psikolojik travmalara ve sosyal dışlanmaya yol açabilmesinin yanı sıra, aynı zamanda siber taciz ve ısrarlı takip suçlarının bir parçası olarak da belirlenebilmektedir. Bu bağlamda, siber takip eylemleri sırasında elde edilen özel görüntülerin rıza dışı yayınlanması, ısrarlı takip suçunun nitelikli hâli olarak değerlendirilebilecek veya bazı ülkelerde bağımsız bir suç tipi olan cinsel içerikli görüntülerin rızaya aykırı ifşası suçunu da oluşturabilecektir.[93]

Bu tür eylemler, genellikle sona ermiş bir ilişkinin ardından failin elinde kalan özel görüntü veya videoları mağduru cezalandırmak ya da utandırmak amacıyla ifşa etmesiyle ortaya çıkmaktadır. Bu eylemde mağdurun cinsel dokunulmazlığı ve mahremiyet hakkı ihlal edilmektedir.[94] Bu eylem, ısrarlı takibin bir "aracı" yahut "aşaması" olarak değerlendirilebileceği gibi, bağımsız bir suç tipi olarak da anlaşılabilir.[95]

**5. Deepfake Taciz**

Deepfake taciz, yapay zekâ ve makine öğrenimi tekniklerinin kullanımıyla, bir kişinin yüzünün veya sesinin, rıza dışı bir şekilde, genellikle pornografik yahut itibar zedeleyici nitelikteki içeriklere sahip başka bir videoya entegrasyonu olarak

---

92 Ibid.

93 Tamer Soysal, 'Sanal Gerçeklik ve Artırılmış Gerçeklik Uygulamalarının Ceza Hukuku Üzerindeki Olası Etkileri Üzerine Bir Deneme' [2023] Türkiye Adalet Akademisi Dergisi 169; Ali Emrah Bozbayındır ve Murat Özok, 'Alman ve İtalyan Ceza Hukukunda Israrlı Takip Suçu' [2022] Galatasaray Üniversitesi Hukuk Fakültesi Dergisi 295.

94 Yargıtay "İntikam Pornosu" olarak adlandırılan rıza dışı ifşa eylemlerini ağırlıklı olarak TCK m. 134/2 ve TCK m. 136 maddeleri çerçevesinde ele almaktadır. Failin, mağdura ait özel videoları mağdurun ve ailesinin rızası dışında Facebook gibi platformlarda yayımlaması, TCK m. 134/2 kapsamında özel hayatın gizliliğini ihlal suçu olarak cezalandırılmaktadır (Yar. 12. CD., 2014/2926 E., 2014/19496 K.) Yargıtay, müstehcen içerikli görüntülerin ifşasında hangi maddenin uygulanacağı konusunda "özel hüküm" ilkesini gözetmektedir. Bir kararda Yargıtay, verileri hukuka aykırı olarak verme suçundan (m. 136) kurulan mahkumiyeti uygun bulurken; benzer nitelikteki başka vakaların özel hayatın gizliliğini ihlal kapsamında değerlendirilmesi gerektiğini, şikâyet yoksa düşme kararı verilmesi gerektiğini hatırlatmıştır (Yar. 12. CD., 2016/296 E., 2016/8375 K.) (Maviş, 2021). Genel eğilim, görüntünün içeriği "özel hayatın gizliliği" alanına giriyorsa m. 134'ün uygulanması yönündedir. Benzer yöndeki Yargıtay kararları için bakınız. 12. CD., E. 2013/25593 K. 2014/165 T. 13.1.2014; 12. CD., E. 2013/2773 K. 2013/26643 T. 25.11.2013; 12. CD., E. 2012/22781 K. 2013/22719 T. 7.10.2013.

95 Çalışkanlar Aşılıoğlu (n 34) 18.

tanımlanır. Bu teknolojiyle üretilen sahte görseller veya videolar, mağduru itibarsızlaştırmak, onu aşağılamak veya tehdit etmek amacıyla kullanılabilir; çünkü bu durum, siber tacizin en ileri ve yıkıcı biçimlerinden birini temsil etmektedir.[96] Bu tür taciz, genellikle bireyin kişisel ve profesyonel yaşamında ciddi tahribatlara yol açabilmekle birlikte, mağdurların kamuoyundaki imajını geri dönülemez biçimde zedeleyebilmektedir.

Özellikle, deepfake tacizinin ısrarlı takiple bağlantısı, bu tür manipüle edilmiş içeriklerin mağdura veya mağdurun çevresine sürekli olarak gönderilmesi yoluyla rahatsızlık yaratılması ve psikolojik baskı oluşturulması durumunda ortaya çıkmaktadır. Deepfake içeriğin intikam amacıyla oluşturularak yayılması hem siber taciz hem de rıza dışı pornografi bağlamında değerlendirilebilmektedir.[97] Deepfake tacizinin gerçekleştirilme şekline bakıldığında, failin mağdurun gerçek görüntüsüne sahip olmasa bile, onun fiziksel özelliklerini kullanarak sahte ama gerçekçi medya içerikleri oluşturduğu görülmektedir. [98] Klasik siber tacizden temel farkı, söz konusu eylemin esasını 'teknolojik manipülasyon' (yapay zekâ) teşkil etmesidir. Bu bağlamda, mağdurun fiilen bulunmadığı bir ortamda varmış gibi temsil edilmesiyle ortaya çıkan bu saldırı, ispatı güç ve etkisi çok daha kalıcı bir siber şiddet türü olarak nitelendirilmelidir.

### 6. Uygulamada Karşılaşılan Teknolojik Sorunlar

Bilişim sistemleri kullanılarak israrlı takip suçunun işlenmesi, bu suçun geleneksel yöntemlere kıyasla daha karmaşık, anonim ve mağdur üzerinde sürekli bir baskı oluşturacak bir düzeye ulaşmasına yol açmıştır.[99] Zira dijital dönüşümle birlikte fail, mağdurun karşısına fiziksel olarak çıkmak yerine, bilişim sistemlerinin sağladığı kolaylıklardan faydalanarak mağdurun yaşam alanını mekânsal ve zamansal sınırlamalardan bağımsız bir şekilde kontrol edebilmektedir.[100] Günümüzde yapay zeka ile üretilen sahte içeriklerin (deepfake) artışı, GPS tabanlı casus yazılımlar kullanılarak konum takibi yapılması ve IoT cihazlarının gözetleme araçlarına dönüşmesi, ceza adaleti sisteminde ciddi kanıt toplama ve tipiklik belirleme sorunlarına yol açmaktadır.[101]

---

96 Soysal (n 96) 188.

97 Beşir Babayiğit, 'Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi Ve De Lege Ferenda Öneriler' (2021) 25 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 655; Yargıtay 12. Ceza Dairesi, 11.09.2024 tarihli, 2024/167 E. ve 2024/4106 K. sayılı kararı, TCK m. 123/A (ısrarlı takip) maddesinin yürürlüğe girmesinden önceki eylemleri kapsasa da mahkemenin dijital platformlardaki süreklilik arz eden taciz eylemlerini ısrarlı takip olarak nitelendirme iradesini ortaya koyması bakımından kritiktir , Yine Yargıtay 15. Ceza Dairesi, 31.05.2016 tarihli, 2014/3867 E. ve 2016/5587 K. sayılı kararı da bilişim sistemleri aracılığıyla gerçekleştirilen müdahalelerin ve bu sistemlerin taciz/takip amaçlı kullanılmasının hukuki nitelemesine dair temel bir karardır.

98 Soysal (n 96) 189.

99 Güneş (n 3) 16.

100 Panda (n 11) 112.

101 'Artificial Intelligence: Technologies, Applications, and Challenges - Google Kitaplar', n.d. [Erişim: 6 Mayıs 2026].

Bu süreçte dijital şiddet, fiziksel şiddetin bir uzantısı olarak ortaya çıkarken, teknik imkanların failin kimliğini gizlemesini kolaylaştırması ve sınır ötesi eylemlerin yetki sorunlarına yol açması, mevcut soruşturma yöntemlerinin teknolojik gelişmelere ayak uyduracak şekilde güncellenmesi gerektiğini göstermektedir.[102] Bu bölümde, uygulamada karşılaşılan teknolojik engeller ve yeni nesil izleme yöntemlerinin hukuki yönlerinin ayrıntılı bir şekilde incelenmesi amaçlanmaktadır.

### D. Yapay Zekâ Destekli Takip

Yapay zekâ teknolojilerindeki hızlı gelişim, ısrarlı takip suçunun işleniş biçimlerini esaslı şekilde dönüştürmüş ve dijital şiddetin çok daha sofistike bir boyuta evrilmesini sağlamıştır. Bu teknolojiler, failin fiziksel varlığına veya sürekli manuel müdahalesine gerek kalmaksızın mağdur üzerinde kesintisiz bir baskı kurmasına olanak tanırken, hukuk sistemi açısından "tespit edilebilirlik" ve "ispat" gibi temel sorunların ortaya çıkmasına yol açmaktadır.[103]

#### 1. Deepfake ve Dijital Manipülasyon Sorunu

Yapay zekâ ile desteklenen izleme sistemlerinin en tehlikeli örneklerinden biri, deepfake teknolojisidir. Fail, mağdurun rızası dışında elde ettiği görselleri veya ses kayıtlarını yapay zekâ algoritmalarıyla manipüle ederek sahte pornografik içerikler (deepnude) veya itibar zedeleyici videolar üretebilmektedir.[104] Bu içeriklerin ısrarlı takip kapsamında bir "temas kurma" aracı olarak kullanılması, mağdurda yaratılan korku ve endişeyi derinleştirmektedir.[105] Ancak söz konusu içeriklerin "sahte" karakteristiği, bilişim suçları ile ısrarlı takip arasındaki sınırın muğlaklaşmasına sebebiyet vermekte; ekseriyetle eylem yalnızca "özel hayatın gizliliğini ihlal" kapsamında değerlendirilerek takibin sürekliliğinin göz ardı edildiği düşünülmektedir.[106]

#### 2. Otomatik Botlar ve "Israr"ın Mekanizasyonu

Yapay zekâ tabanlı botlar aracılığıyla, failin doğrudan ileti gönderme eylemine gerek duyulmaksızın, mağdura farklı platformlar üzerinden kısa zaman dilimlerinde binlerce mesajın iletilmesi mümkün hale gelmektedir.[107]

---

102 Yılmaz İmret (n 6) 25.

103 Dülger (n 1) 34; Gürleyen (n 46) 12.

104 Ali Murat Kırık ve Vahdet Özkoçak, 'Medya ve İletişim Bağlamında Yapay Zekâ Tarihi Ve Teknolojisi: Chatgpt Ve Deepfake İle Gelen Dijital Dönüşüm' [2023] Karadeniz Uluslararası Bilimsel Dergi 73.

105 Jennifer Laffier ve Aalyia Rehman, 'Deepfakes and Harm to Women' (2023) 3 Journal of Digital Life and Learning 1.

106 Soysal (n 96); Mustafa Evren Berk, 'Dijital Çağın Yeni Tehlikesi "Deepfake"' (2020) 16 OPUS Uluslararası Toplum Araştırmaları Dergisi 1508.

107 Esraa Alomari ve diğerleri, 'Botnet-Based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art' (2012) 49 International Journal of Computer Applications 24; Barış Yetkin, 'Siyasal İletişimde Bilişimsel Propaganda: Türkiye'de 23 Haziran 2019 İstanbul Yerel Seçimleri ve Botlar, Cyborglar, Troller' (2020) 2020 İletişim Kuram ve Araştırma Dergisi 24.

Fail tarafından söz konusu botların kullanıma sunulduğunun ispatlanması teknik takip ve IP tespiti süreçlerinin karmaşıklığını artırmaktadır. Botlar aracılığıyla gerçekleştirilen bu yoğun iletişim, failin manuel eylemlerini taklit ettiğinden "ısrar" kriterini karşılarken, failin "bu eylemin kendisi tarafından yapılmadığı, bir sistem hatası veya üçüncü bir tarafın yazılımı sonucu meydana geldiği" yönündeki savunmalarına dayanak sağlayabilir.[108]

Modern yapay zekâ algoritmaları, sosyal medya platformlarının standart taciz filtrelerini bertaraf etmek amacıyla, mesaj içeriklerini sürekli olarak değiştirme (paraphrasing) suretiyle mağdura erişimini sürdürebilmektedir.[109]

**3. Veri Kazıma ve Profilleme**

Yapay zekâ, çevrimiçi cinsiyete dayalı şiddetin tespiti ve azaltılmasına yönelik olarak davranışsal analiz mekanizmaları vasıtasıyla mağdurun dijital ayak izlerini analiz etme olanağını sağlamaktadır.[110] Fail, bu profil sayesinde mağdurun bir sonraki adımını öngörebilmekte ve takibini bu verilere dayanarak çok daha stratejik bir şekilde sürdürmektedir. Bu durum, mağdurun kendisini sadece sanal dünyada değil, fiziksel dünyada da sürekli izlendiği hissini uyandırarak suçun sonucu olan "ciddi huzursuzluk" ve "yaşam tarzının değişmesi" hallerini kaçınılmaz kılmaktadır.[111]

**4. Kimliksizleştirme ve Anonimlik**

Yapay zekâ araçları, failin gerçek kimliğini gizleme eylemini (proxy kullanımı, otomatik hesap oluşturma gibi yöntemlerle) kolaylaştırmakta, bu durum ise kolluk kuvvetlerinin failin tespitini zorlaştırdığı kabul edilmektedir. Mağdurun, tacizcinin kim olduğunu bilememesi veya karşısında bir "algoritma" varmış gibi hissetmesi, yaşanan korku ve endişe (siber terör) boyutunu artırmaktadır.[112] Nitekim uygulamada, söz konusu "hayalet faillerin" tespiti noktasında uluslararası adli yardımlaşma süreçlerinin, teknolojinin dinamik ilerlemesi karşısında yetersiz kaldığı gözlemlenmektedir.[113]

---

108 Hari Venugopalan ve diğerleri, 'FP-Inconsistent: Measurement and Analysis of Fingerprint Inconsistencies in Evasive Bot Traffic' (2024) 1 Proceedings of ACM Conference (Conference'17) (Erişim Tarihi: 6 May 2026); Cebajel Tanan ve diğerleri, 'A Multi-Functional Web Tool for Comprehensive Threat Detection Through IP Address Analysis' [2024] 2024 IEEE Conference on Engineering Informatics, ICEI 2024.

109 Álvaro Huertas-García ve diğerleri, 'Countering Malicious Content Moderation Evasion in Online Social Networks: Simulation and Detection of Word Camouflage' (2022) 3525 CEUR Workshop Proceedings 10 (Erişim Tarih: 6 Mayıs 2026); Peter Jachim, Filipo Sharevski and Paige Treebridge, 'TrollHunter [Evader]: Automated Detection [Evasion] of Twitter Trolls During the COVID-19 Pandemic' (2020) 20 ACM International Conference Proceeding Series 59.

110 Rahul Manche ve diğerleri, 'Empowering Safe Online Spaces: AI in Gender Violence Detection and Prevention' (2025) 10 Journal of Science & Technology 39.

111 Cihan (n 1) 356; Yılmaz İmret (n 6) 26.

112 Güneş (n 3) 16; Panda (n 11) 112.

113 Dülger (n 1) 34.

**E. Konum Takibi**

Gelişen teknolojiyle birlikte, Küresel Konumlama Sistemi ve Bluetooth tabanlı takip cihazları, failin mağduru fiziksel olarak görmesine gerek kalmadan onun her adımını izlemesine olanak tanıyan en yaygın dijital takip araçları haline gelmiştir.[114] Bu teknolojiler, mağdurun hareket özgürlüğünü kısıtlamakta ve üzerinde kesintisiz bir gözetim baskısı tesis etmektedir. Bununla birlikte, Türk Ceza Kanunu'nun 123/A maddesi çerçevesinde söz konusu eylemlerin hukuki nitelendirilmesi, bilhassa uygulamada, teknolojik ve hukuki mahiyette çeşitli sorunları ihtiva etmektedir.

**1. "Fiziken Takip" ve Uzaktan Gözetleme Ayrımı**

TCK m. 123/A'da suçun seçimlik hareketlerinden biri "fiziken takip etmek" olarak düzenlenmiştir. Öğretideki temel tartışmalardan biri, failin mağduru bir GPS cihazı veya insansız hava aracı (drone) vasıtasıyla uzaktan izlemesinin bu kapsamda değerlendirilip değerlendirilemeyeceğidir.

Bir görüşe göre, "fiziki takip" terimi, failin fiziksel olarak ve doğrudan mağdurun peşinde olması anlamına gelmelidir; bu çerçevede, failin bulunduğu yerden dijital ağlar aracılığıyla mağdurun yerini izlemesi "fiziki takip" olarak değerlendirilmeyebilir.[115]

Diğer bir görüş, coğrafi sınırları aşan siber takip eyleminin, mağdur üzerinde fiziki takiple eşdeğer (hatta zaman zaman daha yoğun) bir psikolojik etki meydana getirdiğini ileri sürmektedir.[116] Bu açıdan bakıldığında, failin teknolojik araçlar kullanarak mağdurun yerini belirlemesi, modern bir takip yöntemi olarak değerlendirilmelidir.

**2. "Temas Kurmaya Çalışma" Şartının Yarattığı Boşluk**

Bilişim sistemleri aracılığıyla icra edilen ısrarlı takip suçunun unsurları arasında, kanun koyucu tarafından failin mağdurla "temas kurma teşebbüsü" şartı aranmaktadır.[117]

Mağdurun aracına veya çantasına gizlice bir konum takip cihazı yerleştirilip sadece izlenmesi durumunda, mağdurla aktif bir iletişim (mesaj, arama vb.) kurulmadığı sürece bu eylemin "temas kurma" olarak değerlendirilmemesi gerektiği görüşündeyiz.[118]

Mağdurun, gizli takip eylemini fark etmemesi durumunda, "ciddi bir huzursuzluk" veya "güvenlik endişesi"nin ortaya çıkmayacağı varsayımıyla, bu eylem TCK m. 123/A hükmünün kapsamına girmemektedir. Bu durum, failin eyleminin

---

114 Türkoğlu (n 14) 61.

115 Dülger (n 1) 34; Can (n 9) 20.

116 Dülger (n 1) 34.

117 Özar (n 69) 1428.

118 Gündoğdu (n 3) 27.

yalnızca fark edildiği anda (şartlar uygunsa) TCK m. 134 hükmünde düzenlenen "Özel Hayatın Gizliliğini İhlal" suçu kapsamında değerlendirilmesine olanak tanıyarak, ısrarlı takip kurumunun sistematik yapısına zarar vermektedir.[119]

**3. Donanımsal ve Yazılımsal Takip Zorlukları**

Konum takibi iki farklı şekilde gerçekleşmektedir. Bunlardan ilki donanımsal takiptir. Donanımsal takip, fail tarafından mağdurun eşyalarına (çanta, ceket cebi, araç altı) fiziksel bir cihaz yerleştirilmesidir. Cihazların küçülmesi ve pil ömürlerinin uzaması, bunların tespit edilmesini oldukça zorlaştırmaktadır..[120]

İkinci izleme yöntemi ise yazılım tabanlı izleme olarak adlandırılır. Bu yöntemde, mağdurun telefonuna veya tabletine casus yazılımlar yüklenir ve ardından konum bilgisi failin ekranına iletilir.[121] Bu çerçevede, failin mağdurun konum geçmişine erişmesiyle mağdurun günlük alışkanlıklarının analiz edilmesi ve takibin öngörülebilir bir seviyeye taşınması durumu söz konusu olmaktadır.[122]

Dijital anonimlik nedeniyle, konum takip cihazlarıyla işlenen suçlarda suçluyu tespit etmek oldukça güçleşmektedir.[123]

**F. Casus Yazılımlar**

Günümüzde "stalkerware" olarak da adlandırılan casus yazılımlar failin mağdurun rızası olmaksızın cihazına (telefon, tablet, bilgisayar) sızarak onun konumunu, mesajlarını, arama kayıtlarını ve hatta mikrofon/kamera aracılığıyla ortam seslerini takip etmeyi mümkün kılmaktadır.[124] Söz konusu yazılımların kullanımı, TCK m. 123/A hükmünde yer alan ısrarlı takip suçunun tipiklik unsurlarının somut olayda gerçekleşip gerçekleşmediği hususunda uygulamada ciddi hukuki ihtilaflara veya değerlendirmelere neden olmaktadır.

**1. "Temas Kurma" Şartı ile İlgili Tipiklik Sorunu**

TCK m. 123/A hükmü, bilişim sistemleri aracılığıyla işlenen suçlarda failin mağdurla "temas kurmaya çalışmasını" öngörmektedir.[125]

---

119 Can (n 9) 20.

120 Cynthia Fraser ve diğerleri, 'The New Age of Stalking: Technological Implications for Stalking' (2010) 61 Juvenile and Family Court Journal 39.

121 Can (n 9) 21.

122 Amab Kumar Ghosh, 'An Exploratory Study on the Concept and the Form of Stalking as a Cyber Crime' (2021) 4 International Journal of Law Management & Humanities 668.

123 Lazar Stošić ve Aleksandra Janković, 'Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives' (2022) 19 Kultura polisa 82 (Erişim tarih: 7 Mayıs 2026).

124 Yufei Han, Kevin A Roundy ve Acar Tamersoy, 'Towards Stalkerware Detection with Precise Warnings' [2021] ACM International Conference Proceeding Series 957 (Erişim Tarihi: 7 Mayıs 2026).

125 Can (n 9) 22; Dülger (n 1) 35; TCK m. 123/A kapsamında düzenlenen "temas kurmaya çalışmak" seçimlik hareketine dair Yargıtay, eylemin siber ortamda ya da fiziksel araçlarla "ısrarlı" bir iletişim

Casus yazılımlar, doğaları gereği "hayalet modunda" (gizli) faaliyet göstermektedir. Bu durumda, failin mağdurun her adımını izlemesine karşın, mağdur ile doğrudan bir mesaj veya arama yoluyla aktif bir temas kurmaması halinde, söz konusu eylemin ısrarlı takip suçunu mu yoksa yalnızca TCK m. 134'te düzenlenen "Özel Hayatın Gizliliğini İhlal" suçunu mu oluşturacağı hukuki bir tartışma konusu olmaktadır.[126]

Öğretide, mağdurun izlendiğinden haberdar olmadığı ve failin bir iletişim çabasına girmediği durumlar itibarıyla, TCK m. 123/A'da düzenlenen "temas" unsurunun oluşmadığı, dolayısıyla mezkûr eylemlerin ancak bilişim suçları (m. 243-244) kapsamında cezalandırılması gerektiği görüşü kabul edilmektedir.[127]

**2. Çok Fonksiyonlu İhlaller**

Bu bağlamda, casus yazılım kullanımının genellikle tek bir suçla sınırlı kalmadığı, aksine bir suçlar silsilesini teşkil ettiği tespit edilmektedir. Yazılımın mağdurun cihazına yüklenmesi, TCK m. 243 uyarınca "bilişim sistemine hukuka

başlatma iradesi taşıyıp taşımadığına odaklanmaktadır. Özellikle siber takip vakalarında failin mağdurun rızası hilafına kurmaya çalıştığı bu tek taraflı irtibat girişimleri, suçun maddi unsuru olarak kabul edilmektedir. Yargıtay, temas kurma çabasının suç oluşturabilmesi için eylemlerin belirli bir yoğunluğa ve sürekliliğe ulaşması gerektiğini vurgulamaktadır. Yargıtay 12. CD, 25.12.2023 tarih, E. 2023/874, K. 2023/5864: Bilişim sistemleri aracılığıyla gerçekleştirilen takip ve taciz eylemlerinin m. 123/A kapsamında değerlendirilmesine dair güncel ve emsal bir karardır. Yargıtay 12. CD, 24.10.2023 tarih, E. 2023/1760, K. 2023/4352: Bu kararda Yargıtay, iki aylık bir sürede yapılan 6 aramanın, zaman aralığı ve toplam sayı itibarıyla "ısrarlı temas kurma" olarak kabul edilemeyeceğine hükmetmiştir. Yargıtay 12. CD: Mağdurun konuşmak istemediğini beyan etmesine rağmen 7 kez arayan ve mesaj atan sanığın eylemi, huzur ve sükunu bozma/ısrar kriteri (m. 123 temelinde) kapsamında suç sayılmıştır. Yargıtay 4. CD, 09.05.2016 tarih, E. 2016/4715, K. 2016/9234: Temas kurma çabasının "sırf rahatsız etme" kastı ile "ısrarlı" bir şekilde yapılması gerektiğini, aksi halde suçun unsurlarının oluşmayacağını belirtmiştir. Yargıtay kararlarında "temas" kavramı; telefon, SMS, e-posta ve sosyal medya üzerinden gönderilen içerikleri kapsamaktadır. Yargıtay 12. CD, 23.11.2016 tarih, E. 2015/37827, K. 2016/18068: Dijital araçlarla yapılan temaslarda suçun maddi ve manevi unsurlarının belirlenmesine dair bir içtihattır. Yargıtay 4. CD, 12.05.2014 tarih, E. 2012/34217, K. 2014/16130: Mağdurun "Gülçin" olmadığını söylemesine rağmen 2 gün içinde 4 ayrı mesaj gönderilmesini "ısrar" unsuru için yeterli görmüştür. Yargıtay 18. CD, 14.12.2016 tarih, E. 2015/27706, K. 2016/6459: Sanığın tek bir gün içinde (yaklaşık 1 saatlik dilimde) gönderdiği 3 adet mesajın, "ısrar" öğesini oluşturmayacağı ve dolayısıyla temas kurma çabasının bu madde kapsamında cezalandırılamayacağı yönünde bir bozma kararıdır. Yargıtay ve doktrin, temas kurma kriteri açısından şu ayrımı yapmaktadır. Algılanma Şartı: Failin mağdurla temas kurmuş sayılması için, mağdurun bu çabadan (mesajın iletilmesi, çağrının görülmesi vb.) haberdar olması gerekir. Mağdurun sosyal medya hesabını "gizlice" takip etmek veya paylaşımlarını izlemek (stalklamak), aktif bir temas kurma çabası içermediği sürece TCK 123/A kapsamında suç sayılmamaktadır. Üçüncü Kişiler Aracılığıyla Temas: Failin doğrudan değil, mağdurun çevresini veya üçüncü kişileri kullanarak mesaj iletmeye çalışması da «temas kurmaya çalışmak» seçimlik hareketi dahilinde kabul edilmektedir. Özetle Yargıtay; m. 123/A bağlamında «temas kurma»yı sadece sayısal bir tekrar olarak değil, mağdurun iradesini sakatlayan ve onu yaşam tarzını değiştirmeye zorlayan tek taraflı ve ısrarlı bir iletişim girişimi olarak yorumlamaktadır.

126 Dülger (n 1) 35.

127 Cihan (n 1) 358.

aykırı girme" suçunu oluşturduğu kabul edilmektedir.[128] Mesajların ve aramaların takibi, TCK m. 132-133 kapsamında haberleşmenin gizliliğini ihlal fiilini teşkil etmektedir. Mağdurun fotoğraflarının veya rehberinin ele geçirilmesi kişisel verilerin korunması hukukuna aykırılık teşkil etmektedir.[129] Uygulamada ise tüm bu ihlallerin 'ısrarlı takip' amacı altında tek bir ceza ile (fikri içtima) mi yoksa her birinden ayrı ayrı mı (gerçek içtima) cezalandırılacağı hususundaki tartışmalar yargılamaların karmaşıklığını artırmaktadır.[130]

**3. İspat ve Teknik Tespit Zorlukları**

Casus yazılımlar adli makamlar önünde kanıtlanması en zor takip yöntemlerinden biridir. Bu durum, failin tespitini ve eyleminin hukuki vasıflandırmasını zorlaştıran, özel teknik bilgi ve uzmanlık gerektiren adli bilişim incelemelerini kaçınılmaz kılmaktadır.

Birçok casus yazılım, "ebeveyn kontrolü" veya "kayıp cihaz bulma" maskesi altında pazarlanabilmektedir.[131] Fail ise, bu yazılımı mağdurun rızasıyla yüklediğini iddia ederek suç kastını gizleyebilmektedir.

Yazılımlar genellikle verileri anonim sunucular üzerinden faile aktardığı için, trafik bilgilerinin (logs) elde edilmesi ve fail ile cihaz arasındaki bağın kurulması uluslararası istinabe süreçlerini gerektirmekte, bu da soruşturmaları sekteye uğratmaktadır[132].

Yazılım cihazda bulunduğu sürece mağdurun izlenmesi sürmektedir; ancak ceza hukuku bağlamında "ısrar"ın yazılımın yalnızca bir kez yüklenmesiyle mi yoksa failin verileri her kontrol ettiğinde mi gerçekleşmiş sayılacağı konusunda kesin bir açıklık bulunmamaktadır.[133]

**4. Psikolojik Neticelerin Tespiti**

Israrlı takip suçunun oluşması için mağdurda "ciddi bir huzursuzluk" veya "güvenlik endişesi" meydana gelmesi zorunludur.[134]

---

128 Yörük (n 50) 178.

129 Geliş Tarihi ve Melisa Seval Meray, 'Ceza Hukukunda Siber Zorbalık' (2024) 2 Karatekin Hukuk Dergisi 77.

130 Cihan (n 1) 358.

131 Eva-Maria Maier, Leonie Maria Tanczer ve Lukas Daniel Klausner, 'Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental Control Apps' (2025) 2025 Proceedings on Privacy Enhancing Technologies 107 (Erişim Tarihi: 7 Mayıs 2026).

132 Gündoğdu (n 3) 28.

133 Balcı ve Çakır (n 2) 327.

134 Gündoğdu (n 3) 28; Yargıtay ve öğreti, bu iki unsuru suçun tamamlanması için gerçekleşmesi zorunlu "neticeler" olarak kabul etmektedir. Netice Suçu Vurgusu: Israrlı takip suçu, önceki düzenleme olan TCK m. 123'ün aksine (ki m. 123 bir soyut tehlike suçudur), mağdur üzerinde somut bir etkinin doğmasını şart koşar. Madde gerekçesinde, suçun oluşabilmesi için ısrarlı takip fiilinin mağdur üzerinde ciddi bir huzursuzluk oluşturmasının veya kendisinin/yakınlarının güvenliğinden endişe duymasına neden olmasının şart olduğu açıkça belirtilmiştir. Bu durum, her somut olayda

Uygulamada ise, failin somut bir fiziki takip fiilinin mevcut olmaması durumunda dahi, bu "dijital kuşatma" niteliğindeki hâlin mağdur üzerinde meydana getirdiği yıkıcı etki, TCK m. 123/A hükmü kapsamındaki neticenin gerçekleştiğinin bir ispatı olarak kabul edilmelidir.[135]

### G. Metaverse/VR Ortamlarında Takip

Metaverse, kullanıcıların 3D avatarlar aracılığıyla anlık etkileşimde bulunabildikleri, sanal ve artırılmış gerçeklik teknolojilerinin birleşimiyle oluşan bir dijital dünya olarak tanımlanır[136]. Bu mecralar, ısrarlı takip suçunun işleniş biçimini fiziksel dünya ile dijital dünya arasındaki sınırları muğlaklaştırarak dönüştürmektedir; bu durum yeni tipolojik sorunların ortaya çıkmasına neden olmaktadır.[137]

#### 1. "Temas Kurma" ve "Fiziken Takip" Kavramlarının Genişlemesi

Türk Ceza Kanunu'nun (TCK) 123/A maddesi kapsamında suçun gerçekleşmesi için, failin "fiziken takip eylemini gerçekleştirmesi" ya da "bilişim sistemleri aracılığıyla temas tesis etme girişiminde bulunması" gereklidir. Metaverse ortamında bir failin, mağdurun avatarını sürekli takip etmesi, eriştiği sanal odalara dahil olması veya mağdurun avatarına ait kişisel alanı (virtual personal space) ısrarla ihlal etmesi hâlinde, bu tür eylemlerin hukuki nitelemesi ve mahiyeti bir tartışma konusudur.[138] Öğretide, sanal gerçeklik ortamlarında ısrarlı takibin ger-

---

hâkim tarafından ayrıca belirlenmelidir. Yargıtay, sükûn ve huzuru bozan eylemlerin psikolojik etkilerini şu kararlar ışığında değerlendirmektedir: YCGK 2012/1264 E. 2013/42 K.: Bu karar, bu tür suçların yarattığı zararın maddi değil "manevi" ve "psikolojik" olduğunu teyit eder (Havle, 2025). Bu yaklaşım, m. 123/A'daki ciddi huzursuzluk kriterinin tespitinde manevi zararın yeterli görüleceğine işaret etmektedir. YCGK 2014/821 E. 2018/45 K.: TCK m. 123'ün bir soyut tehlike suçu olduğunu vurgularken, yeni ihdas edilen m. 123/A düzenlemesinin bu tehlikenin "ciddi huzursuzluk" gibi somut bir neticeye dönüşmesini aradığını dolaylı olarak ortaya koyar. Yargıtay 4. CD. 2013/30598 E. 2014/32745 K. (12.11.2014): Eylemlerin "sırf huzur ve sükunu bozma" kastıyla yapılması gerektiğini, bu kastın ispatlanamadığı veya eylemin süreklilik arz etmediği durumlarda suçun oluşmayacağını vurgulamaktadır. Yargıtay ve madde gerekçesine göre, bir huzursuzluğun "ciddi" olup olmadığı şu ölçütlere göre tayin edilir: Yaşam Rutininin Bozulması: Mağdurun okul, iş veya konut değiştirmek zorunda kalması ciddi huzursuzluğun en net göstergesi kabul edilir. Güvenlik Algısının Sarsılması: Failin, mağdurun yakınlarının (babasının iş yeri vb.) fotoğraflarını çekip göndermesi gibi eylemler, doğrudan "güvenlik endişesi" yaratan hareketler olarak nitelendirilmektedir. Hâkimin Takdiri: Ciddi huzursuzluk ölçütü, her ne kadar soyut olsa da, hâkim tarafından dosya kapsamındaki deliller ve mağdurun psikolojik durumu gözetilerek belirlenmelidir. Özetle Yargıtay; m. 123/A kapsamında bir cezalandırma için eylemin nicelik (tekrar sayısı) ve nitelik (rahatsız edicilik düzeyi) itibarıyla mağdurun ruhsal bütünlüğünü bozacak seviyeye ulaştığının tespitini zorunlu kılmaktadır.

135 Balcı ve Çakır (n 2) 327.

136 AP Zen ve IM Miraj, 'The Legal Status of Metaverse Law and Its Implementation in Modern Era' [2023] Sustainable Development in Creative Industries: Embracing Digital Culture for Humanities 129 (Erişim Tarihi: 7 May 2026).

137 Pınar Bacaksız, 'Metaverse Ve Sanal Gerçeklik Ortamları Karşısında Ceza Hukuku' (2023) 14 İnönü Üniversitesi Hukuk Fakültesi Dergisi 289.

138 Bacaksız (n 140) 291; Metaverse ortamındaki etkileşimler, mevcut hukuk sisteminde "bilişim

çekleşmesi için fail ve mağdurun fiziksel olarak aynı ortamda bulunmasının bir koşul olmadığı; bilişim sistemleri üzerinden kurulan bu kesintisiz etkileşimin "temas kurma" unsuru kapsamında değerlendirilebileceği kabul edilmektedir.[139]

**2. Psikolojik Etki ve "Varlık" Duygusu**

Sanal gerçeklik teknolojileri, kullanıcıda "orada olma" (presence) duygusunu tetikleyerek yaşanan deneyimin gerçeklik hissinin artışına zemin hazırlamaktadır.[140] Metaverse platformlarında yaşanan taciz ve ısrarlı takip eylemlerinin, mağdur üzerinde fiziksel dünyadaki saldırılara benzer psikolojik ve duygusal travmalar (korku, endişe, huzursuzluk) yarattığı gözlemlenmiştir.[141] Gelişmiş dokunsal (haptik) cihazların kullanımıyla, sanal dünyadaki bir "temas"ın mağdur tarafından fiziksel bir his olarak algılanması, eylemin TCK m. 123/A'daki "ciddi huzursuzluk oluşturma" neticesinin çok daha hızlı gerçekleşmesine ivme kazandırmaktadır.[142]

**3. Anonimlik ve Kullanıcı Tespiti Zorlukları**

Metaverse platformlarının temel problemlerinden birini, faillerin avatarlar ardına gizlenerek anonimliklerini koruyabilmesi oluşturmaktadır.[143] Bir avatarın hangi gerçek kişi tarafından yönetildiğini belirlemek, platform sağlayıcısının iş birliğini, teknik veri analizini ve IP adresi takibini gerektirir.[144] Dijital kanıtların geçici niteliği, "avatarın kontrolünün kendisinde bulunmadığı" veya "eylemin bir sistem hatasından kaynaklandığı" gibi savunmaların yanlışlığını kanıtlamayı oldukça zor hale getirmektedir.[145]

---

sistemleri aracılığıyla işlenen suçlar" kapsamında değerlendirilmektedir. Yargıtay'ın genel stalking ve dijital taciz yaklaşımını yansıtan kararlar şunlardır: Yargıtay 14. Ceza Dairesi, 18.06.2014 tarihli, 2012/11724 E. ve 2014/8294 K. sayılı ilamı: Bilişim araçları kullanılarak gerçekleştirilen cinsel içerikli taciz eylemlerinin, mağdurun rızası hilafına ve süreklilik arz edecek şekilde yapılmasını cezalandırmaktadır (Soysal, 2023). Bu karar, sanal dünyadaki temasların hukuki karşılığına temel teşkil etmektedir. Yargıtay 4. Ceza Dairesi'nin 2021 tarihli kararları (Örn: 04.11.2021, 2021/26383 K.; 18.10.2021, 2021/24687 K.): Bu kararlar, ısrarlı takip suçunun (TCK m. 123/A) temelini oluşturan "ısrar" kriterinin ve mağdur üzerindeki psikolojik etkilerin tespiti açısından emsal kabul edilmektedir.

139 Bacaksız (n 140) 292.

140 Ufuk Çelikcan, 'Eğitimde ve Tıpta Sanal Gerçeklik Uygulamaları: Geçmişten Geleceğe Uzanan Bir İnceleme' (2022) 13 Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi 235.

141 Muhammad Firkan Muhammad Muslim ve Indi Izza Afdania, 'Legal Construction of Criminal Prosecution Against Perpetrators of Rape in the Metaverse' (2024) 1 Peradaban Hukum Nusantara 60.

142 RK Venkatesan ve diğerleri, 'Haptic Feedback in a Virtual Crowd Scenario Improves the Emotional Response' (2023) 4.

143 MA Efremova ve diğerleri, 'Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development' (2025) 3 Journal of Digital Technologies and Law 187 (Erişim tarihi: 7 May 2026).

144 ibid.

145 Kedi Yang ve diğerleri, 'A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse' (2022) 18 IEEE Transactions on Information Forensics and Security 3817; Tayba Al Ali ve diğerleri 'Digital Forensic in A Virtual World; A Case of Metaverse and VR' (2023) 22 European Conference on Cyber Warfare and Security 12.

### 4. Yetki ve Yargı Yetkisi Problemi

Metaverse platformları genellikle merkezi olmayan bir yapı veya farklı ülkelerdeki sunucular aracılığıyla hizmet sunmaktadır. Fail ve mağdurun farklı ülkelerde yer alması durumunda, trafik bilgilerine ulaşım ve adli süreçlerin yürütülmesi için gerekli olan uluslararası adli yardımlaşma yöntemlerinin yavaşlığı, soruşturmaların etkinliğini olumsuz yönde etkileyebilir.[146] Mevcut ceza yasalarının "mekânsal" suç tanımlamaları, coğrafi sınırları olmayan bu sanal dünyadaki eylemleri kapsamakta yetersiz kalmakta ve bu durum, suçlular için bir "cezasızlık alanı" yaratma riskini taşımaktadır.[147]

## H. IoT Cihazlarıyla Gözetleme

Nesnelerin İnterneti, fiziksel nesnelerin birbirleriyle ve ağlarla bağlantılı olduğu, veri toplayıp paylaştığı devasa bir ekosistemi tanımlamaktadır. Akıllı ev sistemlerinden (kamera, termostat, kilit) giyilebilir teknolojilere kadar uzanan bu cihazlar, ısrarlı takip suçunun işlenişinde failin mağduru uzaktan, kesintisiz ve çoğu zaman mağdurun haberi olmaksızın izlemesine imkân sağlamaktadır.[148] Bu durum, TCK m. 123/A kapsamındaki "temas kurma" ve "bilişim sistemi kullanma" kavramlarının sınırlarını zorladığı kabul edilmekle birlikte, sınırlılıkları tartışılmaktadır.[149]

### 1. Pasif İzleme ve "Temas Kurma" Çıkmazı

TCK m. 123/A, bilişim sistemleri üzerinden işlenen suçlarda failin mağdurla "temas kurma' şartını aramaktadır.[150] Nesnelerin İnterneti (IoT) cihazları (örneğin akıllı bir ev termostatı veya ışık sistemi) üzerinden mağdurun evde olup olmadığını izleyen bir failin mağdura herhangi bir mesaj atmadığı veya doğrudan

---

146 Gündoğdu (n 3) 28.

147 Efremova ve diğerleri (n 146) 192; Zen ve Miraj (n 139) 21.

148 Julia Slupska ve Leonie Maria Tanczer, 'Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things' [2021] The Emerald International Handbook of Technology-Facilitated Violence and Abuse 663.

149 Yargıtay, IoT cihazlarının temelini oluşturan uzaktan izleme ve kayıt alma eylemlerini "özel hayatın gizliliğini ihlal" suçu kapsamında değerlendirmektedir: Yargıtay 12. Ceza Dairesi, 2015/9708 E. ve 2016/10986 K. sayılı ilamı: Bu kararda Yargıtay, teknolojik araçlarla gerçekleştirilen gözetleme eylemlerinin özel hayatın gizliliğini ihlal suçunu oluşturduğuna hükmetmiştir. Öğretide, yeni ısrarlı takip düzenlemesiyle birlikte bu tür sistematik gözetleme eylemlerinin artık TCK m. 134 yerine m. 123/A kapsamında cezalandırılması gerektiği savunulmaktadır. Kapı Deliği Kamerası Vakası: Bir apartman dairesinin kapı gözetleme deliğine dışarıdan fark edilmeyecek şekilde yerleştirilen, ses ve görüntü kaydı yapan kamera düzeneğiyle ilgili olayda; Yargıtay sanıkların "güvenlik" savunmasını reddetmiş, karşı dairenin içini de görüntüleyebilen bu IoT benzeri düzeneği özel hayatın gizliliğini ihlal saymıştır. https://www.aa.com.tr/tr/gundem/yargitay-daire-girisine-kamera-yerlestirip-kayit-alan-apartman-yoneticisine-verilen-cezayi-onadi/3734516 / (Erişim Tarihi: 13.05.2026)

150 Özar (n 69) 1430.

etkileşime girmediği sürece, "temas kurma" unsurunun gerçekleşmediği değerlendirilmesi ihtimali bulunmaktadır.[151]

Failin, mağdurun evindeki akıllı kilidin log kayıtlarını inceleyerek eve giriş-çıkış saatlerini takip etmesi, teknik anlamda bir "temas" olmaktan ziyade, bir "izleme" eylemi olarak nitelendirilmelidir. Bu durum, ısrarlı takip suçu yerine yalnızca Türk Ceza Kanunu'nun 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi tehlikesi taşımaktadır.[152]

**2. Kontrol ve Psikolojik Tahakküm**

Nesnelerin İnterneti (IoT) cihazları, failin mağdurun yaşam alanına müdahale etmesine imkân tanıyarak, fiziksel takibe gerek duyulmaksızın 'ciddi huzursuzluğun' vuku bulmasına aracı olmaktadır.[153] Failin akıllı hoparlörler aracılığıyla mağdurun evine seslenmesi, ışıkları aniden açıp kapatması veya akıllı kilitleri mağdurun üzerine kilitlemesi gibi eylemler, mağdurda her an izlendiği ve kontrol edildiği algısının (omnipresence) oluşmasına yol açmaktadır.[154] Bu eylemlerin, mağdurun yaşam tarzını değiştirmesine (örneğin, akıllı cihazları kullanmayı bırakması veya evini terk etmesi gibi) yol açacak kadar ciddi bir baskı unsuru olduğu düşünülmektedir.[155]

**3. Bilişim Sistemi Kavramının Kapsamı**

Bilişim sistemlerinin kullanımı, ısrarlı takip suçunun işleniş yöntemlerinden biri olarak kabul edilmiştir..[156] Öğretide, bilişim sistemi kavramının yalnızca bilgisayar ve telefonlarla sınırlı kalmaması, bunun yerine veri işleme ve iletme yeteneğine sahip tüm Nesnelerin İnterneti (IoT) cihazlarını (örneğin, akıllı saatler, internete bağlı araçlar) kapsayacak şekilde genişletilmesi gerektiği görüşü yaygındır. Bu şekilde bir yorum yapılmadığında, suçun kapsamı teknolojik yenilikler karşısında daralacak ve IoT ile gerçekleştirilen sürekli izlemeler cezasız kalacaktır.[157]

**4. Dijital Delillerin Toplanması ve Adli Bilişim Sorunları**

Nesnelerin İnterneti (IoT) cihazları üzerinden gerçekleştirilen sürekli izleme sürecinin kanıtlanması, geleneksel bilişim sistemlerine kıyasla önemli zorluklar

---

151 Can (n 9) 23.

152 Can (n 9) 23; Gündoğdu (n 3) 29.

153 Isabel Straw ve Leonie Tanczer, 'Safeguarding Patients from Technology-Facilitated Abuse in Clinical Settings: A Narrative Review' (2023) 2 PLOS Digital Health e0000089 (Erişim Tarihi: 7 Mayıs 2026).

154 Eva Penzey Moog ve Danielle C Slakoff, 'As Technology Evolves, so Does Domestic Violence: Modern-Day Tech Abuse and Possible Solutions' [2021] The Emerald International Handbook of Technology-Facilitated Violence and Abuse 643.

155 Bozbayındır ve Özok (n 96) 302.

156 Gündoğdu (n 3) 34; Çoğan (n 17) 33.

157 Taşkın (n 29) 107.

barındırmaktadır.[158] Veriler, esas olarak ilgili cihazın içinde ve bulut tabanlı sunucularda muhafaza edilmektedir.[159] Birçok düşük maliyetli IoT cihazı, kayıtları yalnızca kısa bir süre saklamakta veya bu kayıtların üzerine yazmaktadır; bu durum, failin sürekli eylemlerinin kronolojik olarak kanıtlanmasını zorlaştırmaktadır..[160]Mağdurun, failin kendi adına kayıtlı bir hesabı (örneğin ortak kullanılan bir akıllı ev hesabı) üzerinden izlenildiğini kanıtlamak için bu hesaba erişim sağlaması, bazı durumlarda mağdurun da bilişim suçları kapsamında cezai sorumluluk üstlenmesine neden olabilir.[161]

Sonuç olarak, Nesnelerin İnterneti (IoT) cihazları aracılığıyla gerçekleştirilen gözetim faaliyetleri, fail ile mağdur arasındaki fiziksel ve dijital mesafeyi ortadan kaldırma potansiyeline sahip olsa da, Türk Ceza Kanunu'nun 123/A maddesinde yer alan "temas kurma" ifadesi, bu tür pasif ve sistematik gözetim eylemlerinin cezalandırılmasını engellemektedir..[162]

## II. TÜRK HUKUKU İÇİN REFORM ÖNERİLERİ

Türk Ceza Kanunu'na eklenen 123/A maddesi, ısrarlı takip mağdurlarını koruma konusunda yenilikçi bir adım olarak değerlendirilse de dijital şiddet ve takip teknolojilerinin sürekli değişen yapısı karşısında bazı yapısal ve prosedürel eksiklikler içerdiğini düşünüyoruz. Bu çerçevede, belirtilen eksikliklerin ortadan kaldırılması ve ilgili yasal düzenlemenin dijital çağın dinamikleriyle uyumlu hale getirilmesi amacıyla aşağıdaki reform taslaklarının kapsamlı bir şekilde tartışılması ve değerlendirilmesi gereklidir.

### A. Müstakil Bir "Siber Takip" Düzenlemesi İhtiyacı

Mevcut TCK m. 123/A, bilişim sistemlerini suçun icra edilme biçimlerinden (seçimlik hareket) biri olarak düzenlemektedir. Bununla birlikte, bilişim sistemleri aracılığıyla icra olunan takip eylemlerinin mahiyeti, fiziksel takipten belirgin farklılıklar arz etmektedir.

Öğretide, siber takibin kendine has dinamikleri (anonimlik, mekândan bağımsızlık, verilerin kalıcılığı) nedeniyle ayrı bir fıkra olarak düzenlenmesi veya müstakil bir "Siber Takip" maddesi oluşturulması gerektiği ileri sürülmektedir.[163] Mevcut "temas kurma" şartı, failin mağduru IoT cihazları veya casus yazılımlar

---

158 Saad Alabdulsalam ve diğerleri, 'Internet of Things Forensics – Challenges and a Case Study' 35 (Erişim Tarihi: 7 May 2026).

159 Sungbum Kim ve diğerleri, A Common Architecture-Based Smart Home Hardware Forensics for Scalable Investigations, (2024), doi:10.21203/RS.3.RS-4532459/V1.

160 Alabdulsalam ve diğerleri (n 161) 39.

161 Gündoğdu (n 3) 36.

162 Can (n 9) 24; Dülger (n 1) 35.

163 Dülger (n 1) 38; Can (n 9) 25.

aracılığıyla yalnızca "izlediği" (pasif gözetleme) durumları kapsamamaktadır.[164] Bu bağlamda reform kapsamında "mağdurun rızası olmaksızın dijital araçlarla izlenmesi, konum takibi veya verilerinin sistematik analizi" fiillerinin de suçun maddi unsuruna açıkça dahil edilmesi zorunluluk arz etmektedir.[165]

**B. Koruma Tedbirlerinin Artırılması ve Etkinleştirilmesi**

6284 sayılı Kanun kapsamında verilen koruma kararları çoğunlukla fiziksel alana özgü uygulanmaktadır. Mağdurun şikâyeti üzerine, failin mağdura dijital kanallardan ulaşmasını engelleyen tedbirlerin tatbiki yanında, failin mağdurun verilerine erişimini kısıtlayan "teknolojik erişim yasaklarının" düzenlenmesi gerekmektedir.[166] Adli makamların, şiddete dönüşme potansiyelini değerlendiren dijital risk analiz araçlarını kullanmaları ve yüksek riskli durumlarda failin bilişim sistemlerini kullanmasının adli kontrol olarak denetim altına alınması önerilmektedir.[167]

Anayasa Mahkemesi'nin, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun Ek 6. maddesinde yer alan ve kolluk kuvvetlerine sosyal medya üzerinden "sanal devriye" faaliyetleri yürütme yetkisi tanıyan hükmü iptal etmesi, siber suçlarla mücadele ve özellikle siber ısrarlı takip (cyberstalking) vakalarının önlenmesi noktasında ciddi bir güvenlik açığı oluşturmuştur. Söz konusu iptal kararı, kişisel verilerin korunması ve mahremiyet hakkını temele alsa da dijital suçların anonimlik zırhı arkasına gizlenerek işlendiği günümüz koşullarında kolluğun proaktif müdahale kapasitesini önemli ölçüde zayıflatmıştır.

Israrlı takip suçunun (TCK m. 123/A) temelini oluşturan "ısrar" ve "davranış örüntüsü" kriterlerinin tespiti, ancak failin dijital ayak izlerinin ve kamuya açık platformlardaki sistemli tacizlerinin proaktif bir biçimde izlenmesiyle mümkündür.[168] Sanal devriye yetkisinin kaldırılmasıyla ortaya çıkan hukuki boşluk, adli makamları suçun işlenmesinden sonra devreye giren "reaktif" bir konuma itmiş; bu durum ise özellikle kadına yönelik şiddet vakalarında ısrarlı takibin daha ağır şiddet eylemlerine evrilmesini engelleyecek olan erken teşhis ve proaktif koruma mekanizmalarını sekteye uğratmıştır.[169] Netice itibarıyla, siber alanın "hukuksuz bir mecra" haline gelmemesi için, polisin sanal dünyadaki önleyici faaliyetlerinin mahremiyet dengesi korunarak ancak operasyonel etkinliği de yitirilmeden yasal bir zeminde yeniden tesisi bir zorunluluk arz etmektedir.[170]

---

164 Can (n 9) 25; Gündoğdu (n 3) 36.

165 Dülger (n 1) 38.

166 Panda (n 11) 114; Sarı (n 7) 109.

167 Yılmaz İmret (n 6) 26; Panda (n 11) 114.

168 Ünal (n 48) 555.

169 Sarı (n 7) 110.

170 Dülger (n 1) 42.

**C. Elektronik Uzaklaştırma Tedbirleri**

Geleneksel 'konuta yaklaşmama' kararlarının, dijital ortamda tatbik edilebilirliği ve etkinliği önemli ölçüde azalmaktadır. Bu nedenle, mağdurun dijital mahremiyetini ve güvenliğini temin etmek amacıyla failin belirli dijital platformlara, sosyal medya hesaplarına veya iletişim araçlarına erişiminin kısıtlanması gibi elektronik uzaklaştırma tedbirlerinin yasal bir zemine oturtulması zorunludur.

Failin dijital dünyada mağdurun profillerine, e-posta adreslerine veya dijital "kişisel alanına" (özellikle Metaverse'de) erişimini önleyici yazılımsal bariyerler ile IP tabanlı engelleme mekanizmaları yasal koruma tedbiri olarak ihdas edilmelidir.[171]

Failin mağdurun cihazlarına yüklediği casus yazılımlar (stalkerware) tespit edildiğinde, failin belirli cihazları kullanmasının yasaklanması veya cihazlarının düzenli olarak kontrol edilmesi bir koruma önlemi olarak uygulanabilir.[172]

**D. Dijital Delil Standartlarının Belirlenmesi**

Siber takip davalarında, delillerin geçici olması ve faillerin kimliklerini gizleyebilme olasılığı, ispat sürecini büyük ölçüde zorlaştırmakta ve bu durum, özel standartların belirlenmesini zorunlu kılmaktadır.[173] Ekran görüntüleri, log kayıtları, IoT veri geçmişi ve bulut sunucu dökümlerinin "hukuka uygun elde edilmiş delil" olarak kabul edilme süreçleri daha erişilebilir hale getirilmelidir. Bu bağlamda, adli bilişim uzmanlarının soruşturma aşamasına erken katılımının, bu verilerin özgünlüğünün belirlenmesi için gerekli olduğu kabul edilmektedir. "Uluslararası siber suçlar iş birliği" mekanizmalarının hızlandırılması ve yurt dışındaki sosyal medya veya Nesnelerin İnterneti (IoT) sağlayıcılarından veri elde edilmesi için bu tür verilerin adli süreçlerdeki geçerliliğinin standardizasyonunun zorunlu hale getirilmesi gerekmektedir.[174]

**E. Platform Sorumluluğu ve İş Birliği Yükümlülüğü**

Sosyal medya ve Metaverse platformları, suçların işlenmesi açısından bir "suç mahalli" olarak değerlendirilmektedir. Bu bağlamda, platform yöneticilerinin, ısrarlı takip ve siber taciz olaylarının önlenmesi, tespiti ve delillerin korunması konusunda belirli yasal sorumluluklar üstlenmeleri gerekmektedir.[175] Bunun dışında, platformların, ısrarlı takip ve taciz davranışlarını tespit eden algoritmalar geliştirmesi ve mağdurların bildirimlerine "derhal" (örneğin, 24 saat içinde)

---

171 Bacaksız (n 140) 293; Efremova ve diğerleri (n 146) 193.

172 Slupska ve Tanczer (n 151) 36; Can (n 9) 26.

173 Gündoğdu (n 3) 38.

174 Gündoğdu (n 3) 42; Efremova ve diğerleri (n 146) 192.

175 Şenol Güneci, 'Yeni Nesil Suç Alanı Olarak Metaverse: Hukuki Sınırlar, Sorumluluklar Ve Düzenleme İhtiyacı Sorumluluğu' [2026] Adalet Dergisi 1019.

yanıt verilmesinin yasal bir zorunluluk olarak düzenlenmesi gerekmektedir.[176] Ayrıca, şüpheli takip olaylarında, platformların trafik verilerini adli makamların talebinden önce belirli bir süre boyunca "saklama" yükümlülüğüne sahip olmaları gerekmektedir.[177] Platformların, "gizli izleme" yapan araçları (botlar, casus yazılım entegrasyonları) durdurmamaları durumunda, idari ve hukuki sorumluluklarının belirlenmesi gereklidir.[178]

### F. "Temas Kurma" Şartının "İzleme ve Gözetleme"yi Kapsayacak Şekilde Genişletilmesi

Mevcut düzenlemeye göre, bilişim sistemleri aracılığıyla işlenen suçun gerçekleşmesi, failin mağdurla "temas kurma girişiminde bulunması" şartına bağlıdır.[179] Casus yazılımlar (stalkerware), nesnelerin interneti (IoT) cihazları veya gizli GPS takibi kullanılarak gerçekleştirilen "pasif izleme" faaliyetleri, fail mağdurla doğrudan iletişim kurmadığı sürece suç kapsamına girmemektedir.[180]

Madde metnine "haberleşme araçlarını kullanarak temas kurmaya çalışmak" ifadesinin yanına "veya her türlü teknik araç vasıtasıyla mağdurun hareketlerini izlemek ya da gözetlemek" ibaresinin eklenmesi gerekmektedir.[181] Bu bağlamda, mağdurun bilgisi haricinde icra edilen dijital gözetleme faaliyetlerinin de ısrarlı takip hükmü dâhilinde cezalandırılabilirliğinin sağlanacağı düşünülmektedir.

### G. "Fiziken Takip" Kavramının Teknolojik Gelişmelere Göre Yeniden Tanımlanması

Mevcut yasal düzenlemede yer alan "fiziken takip" ibaresi, fail ile mağdurun aynı fiziksel mekânda bulunması gerekliliğini çağrıştırmaktadır. Metaverse, sanal gerçeklik ortamları ve drone ile yapılan takiplerde fail ile mağdur arasında fiziki bir temas veya yakınlık bulunmamaktadır, ancak mağdur nezdinde oluşturulan baskı, fiziki takip ile eşdeğer bir nitelik arz ettiği değerlendirilmektedir.[182]

"Fiziken" ibaresi yerine "doğrudan veya teknolojik araçlarla dolaylı olarak fiziksel veya sanal yakınlık kurarak takip etmek" ifadesinin tercih edilmesinin daha isabetli olacağı kanaatindeyiz.[183] Söz konusu değişiklik, Metaverse platform-

---

176 Panda (n 11) 114.

177 Gündoğdu (n 3)42.

178 Imane Fouad ve diğerleri, 'Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels' (2018) 2020 Proceedings on Privacy Enhancing Technologies 499; Leyla Keser Berber ve Ayça Atabey, 'Privacy Screening of Online Game Platforms: A Case Study of "Gamecell"' [2020] Annales de la Faculte de Droit d'Istanbul 181.

179 Dülger (n 1) 42.

180 Can (n 9) 27; Gündoğdu (n 3) 44.

181 Dülger (n 1) 42.

182 Dülger (n 1) 45; Bacaksız (n 140) 294.

183 Bacaksız (n 140) 294.

ları üzerinden gerçekleştirilen avatar takipleri ve insansız hava araçları vasıtasıyla icra edilen gözetleme faaliyetlerini tartışmasız biçimde suçun kapsamına dâhil edecektir.

### H. Yeni Nitelikli Haller ve Ağırlaştırılmış Sebeplerin Eklenmesi

Suçun işlenişinde kullanılan yöntemin ciddiyeti ve mağdurun savunmasız durumu dikkate alınarak ceza artırma nedenlerinin genişletilmesi gereklidir. Yapay zekâ araçlarıyla yapılan ısrarlı takip, deepfake içerikler veya otomatik bot sistemleri kullanılarak gerçekleştirildiğinde, cezanın bir kat artırılmasına yönelik bir düzenleme getirilmelidir.[184] Mağdurun cinsel yaşamı, sağlık bilgileri veya özel görüntülerinin baskı ve izleme aracı olarak kullanılması, suçun temel haline göre daha ağır bir cezayı gerektirir.[185] Bir yıldan uzun süren ısrar veya failin aynı mağdura karşı farklı dijital platformları sistematik olarak kullanması "nitelikli hal" olarak tanımlanmalıdır.[186]

### I. Usul Hükümleri ve Dijital Delil Güvenliğinin Sağlanması

Siber takip olaylarının kanıtlanması, dijital delillerin kolayca kaybolabilmesi nedeniyle ciddi zorluklar barındırmaktadır. Bilişim sistemleri üzerinden yapılan ısrarlı takip suçlarında, IP adresi ve trafik bilgilerini (log kayıtları) elde etmek için BTK ve servis sağlayıcılarla yapılan yazışmaların hızlandırılması amacıyla özel bir usul kanunu veya yönetmelik çıkarılması gerekmektedir.[187] Ayrıca, yurt dışındaki bulut sunucularında depolanan IoT verilerinin (örneğin, akıllı ev kayıtları) adli süreçlerde kullanılabilmesi için siber suçlar açısından uluslararası adli yardımlaşma süreçlerinin geliştirilmesi gerekmektedir.[188]

### J. Önleyici Tedbirlerin Dijital Alanda Etkinleştirilmesi

6284 sayılı Kanun kapsamında oluşturulan koruma önlemlerinin, dijital ortamın kendine has koşullarını da tam olarak içermesi gerekmektedir. Fail için sadece fiziksel uzaklaştırma değil, aynı zamanda "mağdurun sosyal medya hesaplarına yaklaşmama, IP tabanlı engelleme veya dijital iletişim araçlarını mağdur

---

184 Cihan (n 1) 358; Güneş (n 3) 18.

185 Cihan (n 1) 358; Dülger (n 1) 45.

186 Dülger (n 1) 46.

187 Gündoğdu (n 3) 46.

188 Pankaj Sharma ve Lalit Kumar Awasthi, 'IoT Forensics in Ambient Intelligence Environments: Legal Issues, Research Challenges and Future Directions' (2024) 16 Journal of Ambient Intelligence and Smart Environments 73; Maria Stoyanova ve diğerleri, 'A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues' (2020) 22 IEEE Communications Surveys and Tutorials 1191.

aleyhine kullanmama" gibi dijital uzaklaştırma emirlerinin daha etkili bir şekilde uygulanması zorunludur.[189]

Failin mağdurun cihazına casus yazılım yüklediği belirlendiğinde, bu yazılımın kaldırılması ve failin bilişim sistemlerini kullanma yetkisinin belirli sürelerle sınırlandırılması adli kontrol tedbiri olarak düşünülmelidir.[190]

### K. "Israr" Kriterine Yönelik Objektif Kriterlerin Belirlenmesi

Uygulamada, 'ısrar' kriterinin nicel olarak belirlenmesindeki mevcut belirsizlik, yargı organları arasında içtihat birliğinin sağlanmasını engellemekte ve bu durum istikrarsızlığa neden olmaktadır.Yargıtay içtihatlarıyla desteklenerek, "ısrar" kavramının yalnızca sayısal bir tekrar (örneğin, üç kez arama) olarak değil, "mağdurun yaşam tarzını değiştirme zorunluluğu hissetmesi" veya "eylemlerin zaman içinde yayılması" gibi niteliksel ölçütlere dayanması gerektiği konusunun mevzuatımızda açık bir düzenlemeyle netleştirilmesi gerekmektedir.[191]

Söz konusu reform paketinin tatbiki ile Türk Ceza Hukuku'nun yalnızca fiziksel alandaki eylemleri değil, aynı zamanda dijital evrenin en ücra köşelerinde vuku bulan davranışları da kapsayıcı nitelikte, bütüncül bir koruma mekanizması tesis edeceği düşünülmektedir.

## SONUÇ

Türk Ceza Kanunu'na 7331 sayılı Kanun ile eklenen "Israrlı Takip" suçu (m. 123/A), bireyin huzur ve sükununu, iç barışını ve hareket özgürlüğünü koruma altına alan hayati bir düzenleme teşkil etmektedir. Bu çalışma kapsamında yapılan incelemeler, suçun geleneksel yöntemlerden ziyade bilişim sistemleri ve modern teknolojiler vasıtasıyla işlenmesinin, klasik ceza hukuku kavramlarını ciddi bir sınavla karşı karşıya bıraktığını ortaya koymuştur.[192] Zira, dijitalleşen dünyada fail ile mağdur arasındaki fiziksel mesafenin ortadan kalkması neticesinde; ısrarlı takip eylemi, mekânsal bağımlılıktan azade, anonim nitelikte ve mağdurun yaşam alanını sürekli kuşatan bir siber şiddet türüne (cyberstalking) dönüşmüştür.[193]

Çalışmanın ikinci bölümünde ayrıntılandırıldığı üzere, yapay zeka destekli manipülasyonlar (deepfake), otomatik botlar, casus yazılımlar, IoT cihazları ve Metaverse gibi sanal evrenler, suç tipinin kanuni tanımında yer alan "fiziken takip" ve "temas kurmaya çalışma" unsurları arasında gri alanların oluşumuna

---

189 Panda (n 11) 114; Sarı (n 7) 110.

190 Setyo Amirullah ve Sodikin Sodikin, 'The Principle of Legality vs. Digital Sentencing Innovation: The Dialectics of Revocation of Internet Access Rights as a Criminal Penalty in Cybercrime Cases' (2026) 7 SIGn Jurnal Hukum 1078.

191 Dülger (n 1) 53; Cihan (n 1) 358.

192 Cihan (n 1) 360; Dülger (n 1) 58.

193 Panda (n 11) 116; Güneş (n 3) 18.

yol açmaktadır.[194] Özellikle failin mağduru pasif olarak, hiçbir mesaj atmadan sadece dijital araçlarla izlemesi, mevcut yasal düzenlemedeki "temas" şartı nedeniyle çoğu zaman cezasızlık riski barındırmakta veya eylemin gerçek ağırlığını yansıtmaktan uzak biçimde, daha hafif suçlar kapsamında ele alınma ihtimalini doğurmaktadır.[195] Bu durumun, mağdurun yaşadığı "ciddi huzursuzluk" ve "güvenlik endişesi" neticelerini karşılamakta yetersiz kaldığı kanaatini taşımaktayız.[196]

Bu teknolojik ve hukuki darboğazların aşılması için çalışmamızda sunulan reform önerileri hayati önem taşımaktadır. Türk hukuku için önerdiğimiz temel değişiklikler şu şekilde özetlenebilir:

Tanımsal Genişleme: TCK m. 123/A'daki "temas kurma" şartı, pasif izleme ve gözetleme eylemlerini de kapsayacak şekilde güncellenmeli ve "fiziken takip" kavramının Metaverse ve VR dünyasındaki sanal yakınlığı içerecek biçimde genişletilmesi gerekmektedir.[197]

Müstakil Siber Düzenleme: Siber takibin kendine has dinamikleri göz önüne alınarak, ağırlaştırılmış bir nitelikli hal veya müstakil bir fıkra düzenlenmesi gerekmektedir.[198]

Teknolojik Koruma Tedbirleri: 6284 sayılı Kanun kapsamındaki tedbirler, "elektronik uzaklaştırma" ve "dijital geo-fencing" gibi failin sanal ortamdaki erişimini kısıtlayan yenilikçi müeyyideler ile takviye edilmesi gerekmektedir.

Usul ve İspat Standartları: Dijital delillerin uçuculuğu karşısında, platform sağlayıcılarının iş birliği yükümlülüğü artırılmalı ve adli bilişim süreçlerini hızlandıracak usulî kolaylıklar sağlanmalıdır.

Sonuç olarak, ısrarlı takip suçu yalnızca fiziki takibat eylemi olarak algılanan bir durum olmaktan çıkıp, mağdurun yaşam tarzını zorla değiştiren sistematik bir hak ihlalidir.[199] Bu bağlamda, ceza adaleti sisteminin, failin kullandığı yapay zeka ve IoT gibi teknolojik araçların gerisinde kalmaması; mağdurun hem fiziksel hem de dijital dünyadaki huzurunu teminat altına alacak dinamik ve vizyoner bir yasal çerçeve ile olanaklıdır.[200] Önerilen reformların hayata geçirilmesi, Türkiye'nin dijital şiddetle mücadeledeki kararlılığının pekiştirecektir ve ceza normlarının teknolojik gelişim karşısındaki caydırıcılığının muhafazasını sağlayacaktır.

194 Bacaksız (n 140) 294; Soysal (n 96) 192.

195 Can (n 9) 28.

196 Gündoğdu (n 3) 48.

197 Bacaksız (n 140) 296.

198 Güneş (n 3) 18.

199 Cihan (n 1) 360; Yılmaz İmret (n 6) 16.

200 Dülger (n 1) 59.

**KAYNAKÇA**

Alabdulsalam S ve diğerleri, 'Internet of Things Forensics – Challenges and a Case Study' 35 <https://doi.org/10.1007/978-3-319-99277-8_3> (Erişim Tarihi: 7 Mayıs 2026)

Ali T Al ve diğerleri, 'Digital Forensic in A Virtual World; A Case of Metaverse and VR' (2023) 22 European Conference on Cyber Warfare and Security 12 <https://doi.org/10.34190/ECCWS.22.1.1149> (Erişim Tarihi: 7 Mayıs 2026)

Alıcı M, 'Özel Hayatından Dolayı Memura Disiplin Cezası Verilebilir Mi?' (2019) 5 Gümrük ve Ticaret Dergisi 44 <https://dergipark.org.tr/tr/pub/gumrukticaret-dergisi/article/722635> (Erişim Tarihi: 4 Mayıs 2026)

Almarabeh H ve Sulieman A, 'The Impact of Cyber Threats on Social Networking Sıtes' (2019) 10 International Journal of Advanced Research in Computer Science 1 <https://doi.org/10.26483/IJARCS.V10I2.6384> (Erişim Tarihi: 3 Mayıs 2026)

Alomari E ve diğerleri, 'Botnet-Based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art' (2012) 49 International Journal of Computer Applications 24 <https://doi.org/10.5120/7640-0724> (Erişim Tarihi: 6 Mayıs 2026)

Amirullah S ve Sodikin S, 'The Principle of Legality vs. Digital Sentencing Innovation: The Dialectics of Revocation of Internet Access Rights as a Criminal Penalty in Cybercrime Cases' (2026) 7 SIGn Jurnal Hukum 1078 <https://doi.org/10.37276/SJH.V7I2.553> (Erişim Tarihi: 7 Mayıs 2026)

'Artificial Intelligence: Technologies, Applications, and Challenges - Google Kitaplar' <https://books.google.com.tr/books?hl=tr&lr=&id=hJsIEQAAQBAJ&oi=fnd&pg=PP1&dq=Computer+Science+%26+Information+Technology+169+Artificial+Intelligence+and+Applications&ots=JqjC6P3ME4&sig=6NyxXRP9EmZSHNS2ZEM-mk1RbkU&redir_esc=y#v=onepage&q&f=false> (Erişim Tarihi: 6 Mayıs 2026)

Ayas Ö ve Mutlu N, 'Siber Ortamda Kadınlara Karşı Gerçekleşen Israrlı Takip Suçunun Eleştirel Analizi' *Cinsiyet Bağlamında Hukuka Eleştirel Bakış Sempozyumu* (Atılım Üniversites, 2024) <https://www.researchgate.net/publication/394844763_Siber_Ortamda_Kadinlara_Karsi_Gerceklesen_Israrli_Takip_Sucunun_Elestirel_Analizi-Tam_Metin> (Erişim Tarihi: 22 April 2026

Babayiğit B, 'Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler' (2021) 25 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 655 <https://doi.org/10.34246/AHBVUHFD.1018877> (Erişim Tarihi: 4 Mayıs 2026)

Bacaksız P, 'Metaverse ve Sanal Gerçeklik Ortamları Karşısında Ceza Hukuku' (2023) 14 İnönü Üniversitesi Hukuk Fakültesi Dergisi 289 <https://doi.org/10.21492/inuhfd.1187521>

Balcı M ve Çakır K, 'Israrlı Takip Suçu (TCK m. 123/A)' (2022) 10 Kadir Has Üniversitesi Hukuk Fakültesi Dergisi 323

Başar D. ve Uğurlu NS, 'Israrlı Takip: Tanımı ve Sosyal Psikolojik Değişkenler Ile İlişkileri' (2021) 24 Türk Psikoloji Yazıları 22 https://search.trdizin.gov.tr/tr/yayin/detay/507473/israrli-takip-tanimi-ve-sosyal-psikolojik-degiskenler-ile-iliskileri (Erişim Tarihi: 7 Mayıs 2026)

Berber LK ve Atabey A, 'Privacy Screening of Online Game Platforms: A Case Study of "Gamecell"' [2020] Annales de la Faculte de Droit d'Istanbul 181 <https://doi.org/10.26650/ANNALES.2020.69.0007> (Erişim Tarihi: 7 Mayıs 2026)

Berk ME, 'Dijital Çağın Yeni Tehlikesi "Deepfake"' (2020) 16 OPUS Uluslararası Toplum Araştırmaları Dergisi 1508 <https://doi.org/10.26466/OPUS.683819> (Erişim Tarihi: 6 Mayıs 2026)

Boz Çelik AT, 'Türk Ceza Hukukunda Israrlı Takip Suçu' (YayımlanmamışYüksek Lisans Tezi, Gaziantep Üniversitesi 2025)

Bozbayındır AE ve Özok M, 'Alman ve İtalyan Ceza Hukukunda Israrlı Takip Suçu' [2022] Galatasaray Üniversitesi Hukuk Fakültesi Dergisi 295 <https://rayp.adalet.gov.tr/resimler/1/dosya/insan-haklari-ep02-03-202115-14.pdf>

Çalışkanlar Aşılıoğlu A, 'Kadına Yönelik Şiddet Türlerinden Takip : 6284 Sayılı Kanun ve Türk Ceza Kanunu Önleme ve Koruma' (Yayımlanmamış Yüksek Lisans Tezi, Trakya Üniversitesi 2024)

Can BE, 'Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Yaşar Üniversitesi 2023).

Çelebi Dağ B, 'Israrlı Takip ile Yetişkin Ebeveyn Kabul-Ret Algısı Arasındaki İlişkide Kişilik Bozukluklarının Aracı Rolü' (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Gedik Üniversitesi 2022)

Çelikcan U, 'Eğitimde ve Tıpta Sanal Gerçeklik Uygulamaları: Geçmişten Geleceğe Uzanan Bir İnceleme' (2022) 13 Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi 235 <https://doi.org/10.24012/DUMF.1097748> (Erişim Tarihi: 7 Mayıs 2026)

Cihan A, 'Türk Ceza Hukuku Bağlamında Israrlı Takip Suçu (TCK Md. 123_A)' (2023) 13 Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi 339

Çoğan MF, 'Türk Hukukunda Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Erzincan Binali Yıldırım Üniversitesi 2024)

Demir G, 'Ekranın Ötesindeki Gençlik: Dijital Medya Ve Gençlik Söylemlerine Eleştirel Bir Yaklaşım' (2025) 5 Journal of Communication Science Researches 253 <https://doi.org/10.5281/zenodo.16786142> (Erişim Tarihi: 3 Mayıs 2026)

Demirdağ H, 'Sosyal Medya Kullanımı ve Dijital Bir Hastalık Olarak Stalking' (Yayımlanmamış Yüksek Lisans Tezi, Bolu Abant İzzet Baysal Üniversitesi 2025)

Demirkale S, 'Israrlı Takip Suçu' (Yayımlanmamış Yüksek Lisans Tezi, Hasan Kalyoncu Üniversitesi 2024)

Dülger MV, 'Normatif Düzenleme Açısından Israrlı Takip Suçu' (2023) 8 İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 21 https://dergipark.org.tr/tr/pub/iauhfd/article/1283800 (Erişim Tarihi: 3 Mayıs 2026)

Duman N, Öçalan Hİ ve Çoban İ, 'Partner Israrlı Takibi Veya Stalklama: Mağdur ve Saldırgan Karakteristikleri ve Stalklama Taktikleri' (2023) 7 Yaşam Becerileri Psikoloji Dergisi 33 https://doi.org/10.31461/ybpd.1291096 (Erişim Tarihi: 3 Mayıs 2026)

Durmuş B ve Eyüboğlu D, 'Çocuklarda Ekran ve Sosyal Medya Bağımlılığı' (2025) 47 Osmangazi Tıp Dergisi 65 https://doi.org/10.20515/otd.1749275 (Erişim Tarihi: 3 Mayıs 2026)

Efremova MA ve diğerleri, 'Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development' (2025) 3 Journal of Digital Technologies and Law 187 <https://doi.org/10.21202/JDTL.2025.8> (Erişim Tarihi: 7 Mayıs 2026)

Fouad I ve diğerleri, 'Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels' (2018) 2020 Proceedings on Privacy Enhancing Technologies 499 <https://doi.org/10.2478/popets-2020-0038> (Erişim Tarihi: 7 Mayıs 2026)

Fraser C ve diğerleri, 'The New Age of Stalking: Technological Implications for Stalking' (2010) 61 Juvenile and Family Court Journal 39 <https://doi.org/10.1111/J.1755-6988.2010.01051.X/FULL> (Erişim Tarihi: 24 April 2026

Ghosh AK, 'An Exploratory Study on the Concept and the Form of Stalking as a Cyber Crime' (2021) 4 International Journal of Law Management & Humanities 668

Gündoğdu EG, 'Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Takip Suçu' (Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2025)

Güneci Ş, 'Yeni Nesil Suç Alanı Olarak Metaverse: Hukuki Sınırlar, Sorumluluklar ve Düzenleme İhtiyacı Sorumluluğu' [2026] Adalet Dergisi 1019 <https://doi.org/10.57083/adaletdergisi.1919100>

Güneş A, 'As a Continuity of the Different Forms of Violence: Gender-Based Digital Violence Against Women' (2024) 5 Sosyal Mucit Academic Review 118 <https://doi.org/10.54733/smar.1440636>

Gürleyen Y, 'Türk Ceza Kanunu'nda Israrlı Takip Suçu (TCK M. 123/A)' (Yayımlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2024)

Han Y, Roundy KA ve Tamersoy A, 'Towards Stalkerware Detection with Precise Warnings' [2021] ACM International Conference Proceeding Series 957 <https://doi.org/10.1145/3485832.3485901;PAGE:STRING:ARTICLE/CHAPTER> (Erişim Tarihi: 7 Mayıs 2026)

Havle N, 'Israrın Psikolojik Anatomisi: Yargıtay İçtihatları Işığında TCK Madde 123'ün Sübjektif Unsurları' (2025) 7 Adli Bilimler ve Suç Araştırmaları Dergisi 221

Hekim M, 'Ceza Hukuku Açısından Siber Zorbalık' (2024) <https://katalog.marmara.edu.tr/veriler/yordambt/cokluortam/9D/668242e456a7e.pdf> (Erişim Tarihi: 4 Mayıs 2026)

Huertas-García Á ve diğerleri, 'Countering Malicious Content Moderation Evasion in Online Social Networks: Simulation and Detection of Word Camouflage' (2022) 3525 CEUR Workshop Proceedings 10 <https://arxiv.org/pdf/2212.14727> (Erişim Tarihi: 6 Mayıs 2026)

Jachim P, Sharevski F ve Treebridge P, 'TrollHunter [Evader]: Automated Detection [Evasion] of Twitter Trolls During the COVID-19 Pandemic' (2020) 20 ACM International Conference Proceeding Series 59 <https://doi.org/10.1145/3442167.3442169> (Erişim Tarihi: 6 Mayıs 2026)

Karataş Ş, 'Türk ve Alman Hukukunda Israrlı Takip Suçunun Ceza Genel Teorisi Açısından İncelenmesİ' (2026) 16 Hacettepe Hukuk Fakültesi Dergisi 769

Kelly BD, 'Love as Delusion, Delusions of Love: Erotomania, Narcissism and Shame' (2018) 44 Medical Humanities 15 <https://doi.org/10.1136/MEDHUM-2017-011198> (Erişim Tarihi: 3 Mayıs 2026).

Kılıç A, 'Israrlı Takip Suçu (TCK M. 123/A)' (2022) 15 Suç ve Ceza 529 https://search.trdizin.gov.tr/tr/yayin/detay/1169250/israrli-takip-sucu-tck-m-123a (Erişim Tarihi: 3 Mayıs 2026).

Kim S ve diğerleri, 'A Common Architecture-Based Smart Home Hardware Forensics for Scalable Investigations' <https://doi.org/10.21203/RS.3.RS-4532459/V1> (Erişim Tarihi: 7 Mayıs 2026))

Kırık AM ve Özkoçak V, 'Medya Ve İletişim Bağlamında Yapay Zekâ Tarihi Ve Teknolojisi: Chatgpt ve Deepfake İle Gelen Dijital Dönüşüm' [2023] Karadeniz Uluslararası Bilimsel Dergi 73 <https://doi.org/10.17498/KDENIZ.1308471> (Erişim Tarihi: 6 Mayıs 2026)

'Küresel Günlük Sosyal Medya Kullanımı 2025 | Statista' <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/> (Erişim Tarihi: 8 Mayıs 2026))

Laffier J ve Rehman A, 'Deepfakes and Harm to Women' (2023) 3 Journal of Digital Life and Learning 1 <https://doi.org/10.51357/JDLL.V3I1.218> (Erişim Tarihi: 6 Mayıs 2026))

Maier E-M, Tanczer LM ve Klausner LD, 'Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental Control Apps' (2025) 2025 Proceedings on Privacy Enhancing Technologies 107 <https://doi.org/10.56553/POPETS-2025-0052> (Erişim Tarihi: 7 Mayıs 2026))

Manche R ve diğerleri, 'Empowering Safe Online Spaces: AI in Gender Violence Detection and Prevention' (2025) 10 Journal of Science & Technology 39 <https://doi.org/10.46243/JST.2025.V10.I02.PP39-50> (Erişim Tarihi: 6 Mayıs 2026)

Moog EP ve Slakoff DC, 'As Technology Evolves, so Does Domestic Violence: Modern-Day Tech Abuse and Possible Solutions' [2021] The Emerald International Handbook of Technology-Facilitated Violence and Abuse 643 <https://doi.org/10.1108/978-1-83982-848-520211047> (Erişim Tarihi: 7 Mayıs 2026)

Muhammad Muslim MF ve Izza Afdania I, 'Legal Construction of Criminal Prosecution Against Perpetrators of Rape in the Metaverse' (2024) 1 Peradaban Hukum Nusantara 60 <https://doi.org/10.62193/3AGA8D22> (Erişim Tarihi: 7 Mayıs 2026)

Özar S, 'Israrlı Takip Suçu (TCK m. 123_A) 2' (2022) 71 Ankara Üniversitesi Hukuk Fakültesi Dergisi 1397.

Özbilger Hİ, 'Sosyal Medyada Kişisel Verilerin Korunmasına İlişkin Bir Araştırma' (2025) 7 Kişisel Verileri Koruma Dergisi 35 https://dergipark.org.tr/en/pub/kvkd/article/1633255 (Erişim Tarihi: 7 Mayıs 2026)

Özden AB, 'Türk İş Hukuku Kapsamında Psikolojik Taciz (Mobbıng)' (2018) 5 Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi 22 <https://dergipark.org.tr/tr/pub/asead/article/496209> (Erişim Tarihi: 4 Mayıs 2026)

Özden FC, 'Kadın Üniversite Öğrencilerinde Siber Obsesif Takip İle Travma Stres Bozukluğu ve Suç Korkusu Arasındaki İlişki' (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa 2025).

Özkaya H, 'Israrlı Takip Suçunun Düzenlenmesine İlişkin Kademeli Gelişim' (2023) 97 İstanbul Barosu Dergisi 149.

Öztürk Ü, 'Sanal Ortamda Haksız Rekabet Hâlleri' (2021) 1 Konya Barosu Dergisi 71 <https://dergipark.org.tr/tr/pub/konbarder/article/940762> (Erişim Tarihi: 4 Mayıs 2026)

Paltacı BM, 'Dijital Dünya'nın Tehditleri : Siber Zorbalık Ve Siber İstismar' (2024) 4 Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi 56 <https://doi.org/10.5281/ZENODO.12578849> (Erişim Tarihi: 4 Mayıs 2026)

Panda S, 'Towards a Cyberfeminist Framework for Addressing Gender-Based Violence in Social Media: An Introduction' (2023) <https://doi.org/10.4018/978-1-6684-8893-5.ch008>

Rani NSA ve diğerleri, 'Cyberstalking and Youth Behaviors via Social Media' (2022) 12 International Journal of Academic Research in Business and Social Sciences 1151 <https://doi.org/10.6007/IJARBSS/V12-I4/13014> (Erişim Tarihi: 4 Mayıs 2026)

Reva Z, 'Kadına Şiddetin Görünüş Şekli Olarak Israrlı Takip ve Filmlerde İşlenişi' (2025) 26 Kadın/Woman 2000 61 https://dergipark.org.tr/tr/pub/jws/article/1783112 (Erişim Tarihi: 3 Mayıs 2026)

Reynolds EH and Kinnier Wilson J V., 'Obsessive Compulsive Disorder and Psychopathic Behaviour in Babylon' (2012) 83 Journal of Neurology, Neurosurgery & Psychiatry 199 <https://doi.org/10.1136/JNNP-2011-300455> (Erişim Tarihi: 3 Mayıs 2026)

Sarı C, 'Israrlı Takip Suçunun Kadına Yönelik Şiddetin Önlenmesindeki Önemi' (2025) 0 Terazi Hukuk Dergisi 102.

Şenses Ö ve diğerleri, 'Toplumsal Cinsiyet Bağlamında Siber Takip Üzerine Yapılan Bir Araştırma' (2023) 3 Türkiye Medya Akademisi Dergisi 185 <https://doi.org/10.5281/ZENODO.8378628> (Erişim Tarihi: 23 Nisan 2026)

Şenses Ö ve Aydoğdu Karaaslan İ, 'Sosyal Medyada Stalklamak Üzerine Yapılan Bir Araştırma' (2022) 5 Sosyal, Beşeri ve İdari Bilimler Dergisi 1527 https://doi.org/10.26677/TR1010.2022.1114 (Erişim Tarihi: 3 Mayıs 2026)

Sharma P ve Kumar Awasthi L, 'IoT Forensics in Ambient Intelligence Environments: Legal Issues, Research Challenges and Future Directions' (2024) 16 Journal of Ambient Intelligence and Smart Environments 73 <https://doi.org/10.3233/AIS-220511;ISSUE:ISSUE:DOI> (Erişim Tarihi: 7 Mayıs 2026)

Slupska J ve Tanczer LM, 'Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things' [2021] The Emerald International Handbook of Technology-Facilitated Violence and Abuse 663 <https://doi.org/10.1108/978-1-83982-848-520211049> (Erişim Tarihi: 7 Mayıs 2026).

Solmaz Yiğit E, 'Ergenlerin Bağlanma Stilleri İle Psikolojik İhtiyaçları Arasındaki İlişkide Israrlı Takip Edilmenin Aracılık Rolü' (Yayımlanmamış Yüksek Lisans Tezi, Karamanoğlu Mehmetbey Üniversitesi 2024).

Soygüt BM, 'Kadına Yönelik Erkek Şiddetinin Önlenmesi Bağlamında Stalking (Israrlı Takip) ve Cezasızlık Sorunu' (2020) 5 Çankaya Üniversitesi Hukuk Fakültesi Dergisi 2781.

Soysal T, 'Sanal Gerçeklik ve Artırılmış Gerçeklik Uygulamalarının Ceza Hukuku Üzerindeki Olası Etkileri Üzerine Bir Deneme' [2023] Türkiye Adalet Akademisi Dergisi 169 <https://doi.org/10.54049/TAAD.1231807> (Erişim Tarihi: 4 Mayıs 2026).

Stošić L ve Janković A, 'Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives' (2022) 19 Kultura polisa 82 <https://doi.org/10.51738/KPOLISA2022.19.4R.82SJ> (Erişim Tarihi: 7 Mayıs 2026).

Stoyanova M ve diğerleri, 'A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues' (2020) 22 IEEE Communications Surveys and Tutorials 1191 <https://doi.org/10.1109/COMST.2019.2962586> (Erişim Tarihi: 7 Mayıs 2026).

Straw I ve Tanczer L, 'Safeguarding Patients from Technology-Facilitated Abuse in Clinical Settings: A Narrative Review' (2023) 2 PLOS Digital Health e0000089 <https://doi.org/10.1371/JOURNAL.PDIG.0000089> (Erişim Tarihi: 7 Mayıs 2026).

Tanan C ve diğerleri, 'A Multi-Functional Web Tool for Comprehensive Threat Detection Through IP Address Analysis' [2024] 2024 IEEE Conference on Engineering Informatics, ICEI 2024 <https://doi.org/10.1109/ICEI64305.2024.10912188> (Erişim Tarihi: 6 Mayıs 2026).

Tarihi G ve Meray MS, 'CEZA HUKUKUNDA SİBER ZORBALIK' (2024) 2 Karatekin Hukuk Dergisi 77 <https://doi.org/10.70011/KAHD.1361984> (Erişim Tarihi: 7 Mayıs 2026).

Taşkın ŞC, 'Israrlı Takip Suçu' (2023) 10 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 91 https://doi.org/10.46547/imuhfd.2023.10.1.5 (Erişim Tarihi: 7 Mayıs 2026).

Tulay ME, 'Israrlı Takip Suçunun Suç Teorisi Ile Uyumu Üzerine Bir Değerlendirme' (2024) 14 Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi 57.

Türkoğlu S, 'Türk Ceza Hukuku Açısından Israrlı Takip' (Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi 2019)

Uludağ BC ve Fidan S, 'Rutin Aktiviteler Teorisi Bağlamında Dijitalleşen Dünyada Siber Suç Mağdurları' (2023) 4 Habitus Toplumbilim Dergisi 175 <https://dergipark.org.tr/tr/pub/habitus/article/1258093> (Erişim Tarihi: 4 Mayıs 2026)

Ünal E, 'Israrlı Takip Suçunda Yer Alan Israr Kavramının Hukuki Niteliği ve Suç İçin Öngörülen Yaptırım Özelinde Tehdit Suçuyla İlişkisi Üzerine Bir Değerlendirme' (2024) 9 İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi 549.

Venkatesan RK ve diğerleri, 'Haptic Feedback in a Virtual Crowd Scenario Improves the Emotional Response' (2023) 4 Frontiers in Virtual Reality 1242587 <https://doi.org/10.3389/FRVIR.2023.1242587/TEXT> (Erişim Tarihi: 7 Mayıs 2026)

Venugopalan H ve diğerleri, 'FP-Inconsistent: Measurement and Analysis of Fingerprint Inconsistencies in Evasive Bot Traffic' (2024) 1 Proceedings of ACM Conference (Conference'17) <https://arxiv.org/pdf/2406.07647> (Erişim Tarihi: 6 Mayıs 2026)

Y V, Rathod R ve Kumar R, 'Social Networking Sites in Daily Life: Benefits and Threats' [2022] Artificial Intelligence and Communication Technologies 51 <https://doi.org/10.52458/978-81-955020-5-9-5> (Erişim Tarihi: 3 Mayıs 2026)

Yaldız Ç, 'Yargıtay Kararları Işığında Cinsel Taciz Suçu Ve İncelemesi' (2023) 7 The Journal of Social Science 213 <https://doi.org/10.30520/TJSOSCI.1346873> (Erişim Tarihi: 4 Mayıs 2026)

Yang K ve diğerleri, 'A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse' (2022) 18 IEEE Transactions on Information Forensics and Security 3817 <https://doi.org/10.1109/TIFS.2023.3288689> (Erişim Tarihi: 7 Mayıs 2026)

Yetkin B, 'Siyasal İletişimde Bilişimsel Propaganda: Türkiye'de 23 Haziran 2019 İstanbul Yerel Seçimleri ve Botlar, Cyborglar, Troller' (2020) 2020 İletişim Kuram ve Araştırma Dergisi 24 <https://doi.org/10.47998/IKAD.785151> (Erişim Tarihi: 6 Mayıs 2026)

Yılmaz H ve Kaymaz A, 'KURUMSAL BİR RİSK UNSURU: MOBBİNG (İŞ YERİNDE PSİKOLOJİK TACİZ)' [2016] Denetişim 73 <https://dergipark.org.tr/tr/pub/denetisim/article/240296> (Erişim Tarihi: 4 Mayıs 2026)

Yılmaz İmret H, 'Kadına Karşı Şiddetin Bir Türü Olarak Israrlı Takip Suçu (TCK'nın 123/A Maddesi)' (2024) 11 İstanbul Üniversitesi Hukuk Fakültesi Dergisi 1.

Yörük AB, 'Mevzuatımızda Yeni Bir Suç Tipi: "Israrlı Takip"' (2025) 11 İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi 169 https://dergipark.org.tr/tr/pub/iauhfd/article/1768018 (Erişim Tarihi: 4 Mayıs 2026).

Zen AP ve Miraj IM, 'The Legal Status of Metaverse Law and Its Implementation in Modern Era' [2023] Sustainable Development in Creative Industries: Embracing Digital Culture for Humanities 129 <https://doi.org/10.1201/9781003372486-24> (Erişim Tarihi: 7 Mayıs 2026)