

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

HUKUK FAKÜLTESİ

Konu: Sempozyum Daveti

04.03.2026

Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesinin ev sahipliğinde “**Siber Suçlar Uluslararası Sempozyumu**” başlıklı bir bilimsel etkinlik gerçekleştirilmesi planlanmıştır. Sempozyum oturumları, **21 Ocak 2027** tarihi itibarıyla gerçekleştirilecektir. Sempozyum programının **Kapadokya**’da gerçekleştirilmesine yönelik çalışmalar sürdürülmektedir. Bu çalışmalardan olumlu sonuç alınamaması halinde, program **Ankara**’da gerçekleştirilecektir. Bu husustaki gelişmelerden ilgililer bilgilendirilecektir.

Sempozyum, konuya ilgi duyan bütün yükseköğretim kurumlarının ve ilgili kamu kurumlarının katılımına ve işbirliğine açıktır.

Planlanan Sempozyumda bildiri sunmak isteyen kişilerin, bildiri konusuna ilişkin özet bilgiyi, en geç **30 Nisan 2026** tarihine kadar, Sekretarya adresine e-posta yoluyla göndermeleri gerekmektedir.

Sunulacak olan bildiri metinleri Türkçe, İngilizce veya Almanca olacaktır. Türkçe sunulacak olan bildiriler, yayımlanmak üzere, yazarı/yazarları tarafından ayrıca Almanca veya İngilizce olarak kaleme alınacaktır.

Bildiri özetleri, ön incelemeye tabi tutulduktan sonra, en geç **20 Mayıs 2026** tarihine kadar ilgililere bilgi verilecektir.

Gerekli **hakem** incelemelerinin önceden yapılabilmesini sağlamak için, hazırlanmış bildiri metnlerinin en geç **15 Ekim 2026** tarihine kadar Sekretarya adresine e-posta yoluyla gönderilmesi gerekmektedir.

Bildiri metinleri, Sempozyumda yapılacak tartışmalarla birlikte kitap olarak yayımlanacaktır.

Sempozyumda bildiri sunacak olan kişilere, program sürecinde konaklama imkânı sağlanacaktır. Konaklama imkânı sağlanacak gün sayısına ilişkin bilgi, bildiri sunacak olanlara bilahare bildirilecektir.

Sempozyumda sunulabilecek olan bildirilere ilişkin konular, sayılanlarla sınırlı olmamak kaydıyla, aşağıda sıralanmıştır:

I. Kriminolojik Açıdan Siber Suçluluk ve Önleyici Kolluk Faaliyetleri

- Dünyada ve Türkiye’de **siber suç** eğilimleri ve güncel istatistiklerin karşılaştırmalı biçimde değerlendirilmesi,
 - **Hizmet olarak siber suç (cybercrime-as-a-service)** mefhumu ve ortaya çıkardığı yeni tehdit modelleri,
 - Siber suçlulukla mücadelede uluslararası işbirliği mekanizmaları ve fonksiyonları (Europol, Interpol),
 - **Kritik veri tabanları** bağlamında güvenlik sorunu (e-devlet, enerji, bankacılık, sağlık, ulaşım gibi alanlarda ortaya çıkan siber güvenlik sorunları),
 - **Dezenformasyon, deepfake ve dijital manipülasyon** bağlamında güvenlik sorunları ve bu durumun ortaya çıkardığı yeni tehlikeler, ihdas edilebilecek suç tipleri,
 - **Dijital mecraların çocuklar bakımından ortaya çıkardığı sorunlar** ve bu kapsamda özellikle;
- Online kumar ve bilgisayar oyunlarında “loot box” uygulamaları,
- Online akran zorbalığı,
- Online suç alt kültürü ve birlikte suç işlemeyi teşvik eden grup ve yapılanmalar meselelerinin değerlendirilmesi
- **Dijital iletişim,**
 - **Yapay zekâ** sistemlerinin önleyici kolluk faaliyetlerinde kullanılması,
 - **Ceza adaleti sisteminde kullanılabilecek yapay zeka sistemlerinin eğitilmesi,** yapay zeka sistemlerinin eğitimi için gerekli olan istatistiki bilgiler, kriminolojik araştırmalar ve bu kapsamda Türkiye’nin mevcut durumu,
 - **Kripto varlıkların** suçtan kaynaklanan malvarlığı değerlerini aklama aracı olarak kullanılması ve bu hususta alınabilecek tedbirler,
 - **Kripto varlıkların** suç teşkil eden fiiller bakımından ödeme aracı olarak ya da suç örgütlerinin finansmanı için kullanılması,
 - Siber alanda servis sağlayıcıların ceza sorumluluğu, suç işlenmesinin önlenmesi için ulusal veya uluslararası düzeyde servis sağlayıcılara tahmil edilebilecek yükümlülükler,
 - Siber suçların önlenmesinde kullanılabilecek yeni önleyici kolluk faaliyetleri, bu faaliyetlere yönelik kanuni düzenlemeler ve savunma hakları bakımından ortaya çıkabilecek sorunlar.

II. Siber Suçlar ve Maddi Ceza Hukuku

Siber alanın ve yeni teknolojilerin meydana getirdiği yeni tehditler ve bu bağlamda ortaya çıkan ya da ihdas edilmesi gereken yeni suç tipleri,

İşlenmesi için siber alana ya da yeni teknolojilerin mevcudiyetine ihtiyaç duymamakla birlikte, bu nedenle işlenmesi kolaylaşan ya da daha farklı şekillerde işlenebilir hale gelen suçların siber alanda/dijital mecralarda/bilişim sistemleri marifetiyle işlenmesi sorunu ve bu kapsamda özellikle;

Dolandırıcılık

Kişisel veriler bağlamında işlenen suçlar,

Özel hayatın gizliliği bağlamında işlenen suçlar,

Ticari sır, devlet sırrı gibi **gizli bilgiler** bağlamında işlenen suçlar,

Fikri veya sınai haklar bağlamında işlenen suçlar,

Şans ve bahis oyunları bağlamında işlenen suç ve kabahatler,

Siber zorbalık, çevrimiçi taciz ve dijital şiddet türleri, özellikle kadınlar ve gençler üzerinde artan mağduriyet boyutları,

Deepfake ile pornografik görüntü ve ses üretimi,

Kamera sistemlerinin hacklenmesi yoluyla özel hayatın gizliliğini ihlal,

Kimlik avı (phishing), sosyal mühendislik ve dijital dolandırıcılık pratikleri, SMS/e-posta temelli yaygın saldırı örüntüleri,

Finansal suçlar ve dijital ödeme sistemleri üzerinden gerçekleştirilen dolandırıcılık, mobil bankacılık, sahte yatırım vaatleri ve kripto varlık temelli suç tipleri,

Kripto varlık temelli piramit satış ve dolandırıcılık suçları,

Organize suç ağlarının dijital platformlar üzerinden faaliyet yürütmesi, örgüt içi haberleşmenin ve para transferinin siber alanda sağlanması

Darkweb ekosistemleri, darkweb üzerinde işlenen suçlar; bu kapsamda uyuşturucu madde ticareti, belgede sahtecilik, silah ticareti ve çocuk pornografisi,

İnsan ticareti,

Çevrimiçi içerik ekonomisi ve kayıt dışı dijital gelir modelleri, abonelik temelli içerik üretimi, vergisel uyum ve hukuki düzenleme ihtiyacı,

Dezenformasyon, manipülasyon ve koordineli etki operasyonları,

-Sahte hesaplar, bot ağları ve ücretli yorum/itibar manipülasyonu, troller, dijital kamusal alanın güvenilirliğine yönelik riskler,

-Dijital platformlar üzerinden yasa dışı bahis, kara para aklama ve suç gelirlerinin aklanması, finansal istihbarat ve denetim boyutları, futbol ekonomisine etkileri meselelerinin değerlendirilmesi,

-Mevcut suç tiplerine yönelik olarak; bilişim sistemlerinin ya da yapay zekanın araç olarak kullanılmasının maddi ceza hukuku bakımından anlamı ve bu durumun soyut ve somut cezaların tayinine olası etkileri,

-Yukarıda sayılan bütün suç tiplerine ya da tehdit modellerine yönelik olarak, farklı devletlerin ceza kanunlarındaki hükümlerin değerlendirilmesi,

-Yapay zekâ ve ceza sorumluluğu,

-Otonom sistemler ve ceza sorumluluğu,

-**Otonom silah sistemlerinin** kullanımının savaş hukuku bakımından değerlendirilmesi,

-Dijital mecralar ve **unutulma hakkı**.

III. Siber Suçların Uluslararası Özelliği ve Ceza Hukuku

-**Siber suçların sınır aşan özelliğinin** ceza ve ceza muhakemesi hukuku alanında ortaya çıkardığı sorunlar,

-Siber suçlar bağlamında **uluslararası adli işbirliği**,

-**Siber suçlar ile etkili mücadeleye yönelik olarak akdedilen uluslararası sözleşmeler** ve bu sözleşmelerde taraflara tahmil edilen yükümlülüklerin değerlendirilmesi

-**Delil olarak dijital veriler**; elde edilmesi, kullanılması, değerlendirilmesi, saklanması,

-Yapay zeka ile ses ve görüntü üretiminin, **delillerin sıhhati** bakımından meydana getireceği olası tehlikeler,

-**Kripto varlık transferlerinin** uluslararası alanda takibi,

-**Yapay zekâ** sistemlerinin ceza muhakemesinde delil elde edilmesi veya karar alma süreçlerinde kullanılması,

-**Yapay zekâ** sistemlerinin cezaların infazı sırasında risk ve ihtiyaç değerlendirilmesinde kullanılması,

-**Yapay zeka** sistemlerinin ceza adaleti sisteminde kullanılmasının meydana getirebileceği olası sorunlar ve hak ihlalleri,

-Avrupa Konseyi **Sanal Ortamda İşlenen Suçlar Sözleşmesi**, (Budapeşte, 23.11.2001) (ETS No: 185)

-Birinci Ek Protokol (Strazburg, 28.1.2003) (ETS No: 189)

-İkinci Ek Protokol (Strazburg, 12.5.2022) (CETS No: 224) hakkında değerlendirmeler.

Bildiri Konusunun Belirlenmesinde ve Bildirinin Hazırlanmasında Dikkate Alınabilecek Hususlar:

Sempozyumda, siber suçların bireysel ve toplumsal düzlemdeki kriminolojik arka planı ile devletlerin bu tehditlere karşı geliştirdiği suç politikaları ele alınacaktır. Bildiri konuları yukarıda sayılan konularla sınırlı olmamakla birlikte, hazırlanacak olan bildirilerin konularının sempozyumun tematiği ile uyumlu olması beklenmektedir.

Bildiri içeriklerinde, ülkemizde yürürlükte olan mevzuat ve uygulamayla sınırlı kalınmadan, karşılaştırmalı hukuktaki güncel eğilimlerin, doktriner tartışmaların ve siber suç politikasının bir gereği olarak sunulan yeni *suç ihdası* önerilerinin değerlendirilmesi istenmektedir.

Bildiri sunmak isteyen katılımcıların; siber suç fenomenini sadece hukuki bir ihlal olarak değil, sosyal ve psikolojik bir olgu olarak analiz eden; fail motivasyonları, mağdur tipolojileri ve dijital ortamın suç davranışını tetikleyen dinamiklerini (anonimlik etkisi, siber fırsat yapıları vb.) inceleyen multidisipliner çalışmalar yapmaları beklenmektedir.

Sempozyum konularını ve bu alandaki teknolojik gelişmeleri kavramanın derin uzmanlık bilgisini gerektirmesi dolayısıyla; bildiri sunmak isteyen hukukçuların, bilişim, finans, siber güvenlik, psikoloji, kriminoloji gibi alanlarda uzman olan kişilerle birlikte çalışma yapmaları arzu edilmektedir.

Sempozyum Sekretarya e-posta adresi: sibersuclarsempozyumu2027@gmail.com

Sempozyum Sekretarya sorumlusu: Dr. Efe Can KARABULAT

Prof. Dr. İlhan ÜZÜLMEZ

DEKAN