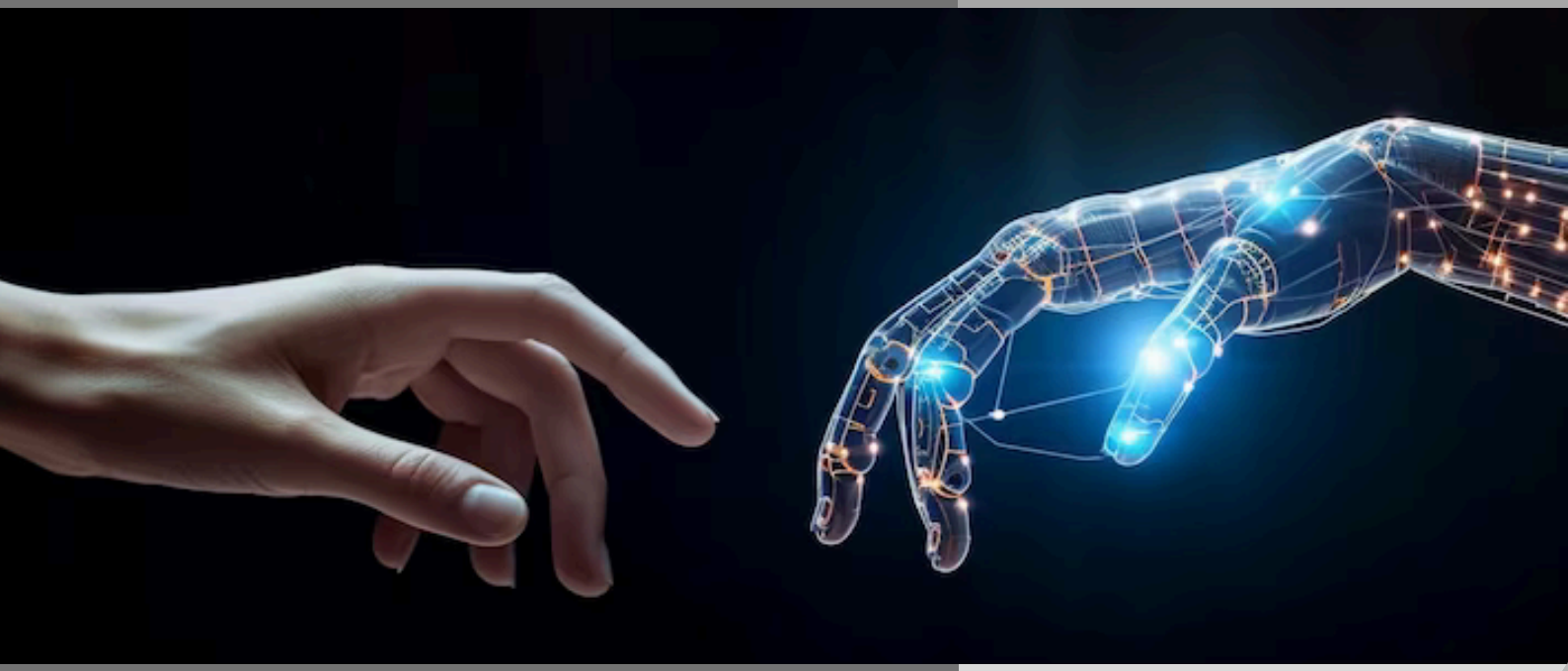
OCAK-MART 2026 | SAYI 21

BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ



BU SAYIMIZDA

BÜLTENİMİZDE

Teknoloji, bizlerin takip edemeyeceği hızda gelişmekte ve hayatımızın ayrılmaz bir parçası haline gelmektedir. Her gün gelişen teknolojiye ayak uydurmak biz hukukçular için zorunlu hale gelmiştir. Yapay zeka, blockchain, fintech, NFT, fikri ve sınai mülkiyet, internet, e-ticaret, kişisel verilerin korunması gibi kavramların insan hakları, ceza hukuku, sözleşmeler hukuku gibi hukukun temel alanlarında incelemek ve bunlar hakkında bilgi sahibi olmak biz hukukçuların bakış açısını geleceğe yönlendirecektir.

Aynı zamanda bu kazanımlar ile hukukçular, bilişim dünyasında yoğun zaman geçiren milyarlarca insanın işlem güvenliğini sağlamak ve dijital anlamda da geleceğe temiz bir dünya bırakmak görevi de üstlenmektedir .

Bu düşünceler ile bizler de bilişim ve hukukun kesiştiği alanlardaki gelişmeleri takip ederek siz değerli okuyucularımıza aktarabilmek, yeni çıkan yasal düzenlemeleri sizlerle buluşturabilmek adına Bursa Barosu Bilişim Hukuku Komisyonu olarak sizlere her ay bülten hazırlıyoruz.

Bilişim hukuku alanında meslektaşlarımızın sizler için hazırladığı makaleleri, haberleri, dizi, film ve kitap önerilerini ve daha birçok içeriği her ay bültenimizden takip edebilirsiniz.

Bültenimizin siz okuyucularımız için bilgi verici olmasını ve okurken keyifli zaman geçirmenizi temenni ediyoruz.

Saygılarımızla.

SADAKAT KART PROGRAMLARINDA KİMLİK DOĞRULAMA SORUNU

KİŞİSEL VERİLERİ KORUMA KURULU'NUN 11.02.2026 TARİHLİ İLKE KARARININ DEĞERLENDİRİLMESİ

AV. BENGİSU AKKAN

1. Giriş

Başta perakende, gıda, kozmetik, teknoloji ve giyim sektörleri olmak üzere birçok işletme tarafından müşteri sadakatini artırmak amacıyla uygulanan sadakat kart programları, son yıllarda veri temelli pazarlama stratejilerinin önemli araçlarından biri haline gelmiştir. Sadakat Kart Programı aracılığıyla tüketicilerin alışveriş alışkanlıkları kayıt altına alınmakta, kişiye özel indirim ve kampanyalar sunulmaktadır. Bununla birlikte söz konusu programlar, kapsamlı kişisel veri işleme faaliyetleri içermesi sebebiyle kişisel verilerin korunması bakımından çeşitli riskleri de beraberinde getirmektedir.

Bu bağlamda Kişisel Verileri Koruma Kurulu, sadakat kart üyeliği bulunan kişilere ait cep telefonu numarası veya sadakat kart numarasının üçüncü kişiler tarafından alışveriş sırasında kullanılmasına ilişkin uygulamaların kişisel veri güvenliği açısından sakıncalar doğurabileceği nedeniyle 11.02.2026 tarih ve 2026/266 sayılı İlke kararı yayımlanmıştır. Kurul tarafından alınan bu karar ile sadakat kart işlemlerinde kimlik doğrulama mekanizmalarının oluşturulması zorunluluğu gündeme gelmiştir.

Bu çalışmada söz konusu İlke Kararı'nın kapsamı, dayandığı hukuki gerekçeler ve uygulamaya muhtemel etkileri kişisel verilerin korunması kanunu çerçevesinde değerlendirilecektir.

2. Sadakat Kart Uygulamalarında Ortaya Çıkan Veri Koruma Sorunu

Sadakat kart programları genellikle bir üyelik sözleşmesi kapsamında oluşturulmakta ve ilgili kişinin şahsi kullanımına özgülenmek suretiyle kişinin cep telefonu numarasını veya sadakat kartı numarasını kasa görevlisine bildirmesiyle uygulama alanı kazanmaktadır. Bu sayede sadakat kartı sahibi yaptığı alışveriş üzerinden indirim ve promosyonlardan faydalanabilmektedir.

Ancak uygulamada sadakat kart sahibi kişiye ait cep telefonu numarasının veya kart numarasının alışveriş sırasında kasa görevlisine sözlü olarak bildirilmesi suretiyle, herhangi bir doğrulama yapılmaksızın sadakat kart avantajlarından yararlanılabildiği görülmektedir. Bu durumda kart sahibinin bilgisi ve rızası olmaksızın üçüncü kişiler tarafından kartın kullanılabilmesi mümkün hale gelmektedir.

Kurul tarafından yürütülen incelemeler sonucunda bu uygulamanın sektörde yaygın olduğu ve çeşitli kişisel veri ihlallerine yol açabileceği tespit edilmiştir. Özellikle sadakat kart üzerinden gerçekleştirilen alışveriş işlemleri sonucunda satın alınan ürün bilgileri, alışveriş tarihi gibi müşteri işlem verilerinin kart sahibi kişinin hesabına işlenmesi, veri kayıtlarının gerçeğe aykırı hale gelmesine neden olabilmektedir. Ayrıca bazı durumlarda alışverişe ilişkin fatura veya benzeri belgelerin sadakat kart sahibi adına düzenlenmesi de söz konusu olabilmektedir.

3. İlke Kararının Hukuki Dayanakları

Kurul, söz konusu uygulamayı değerlendirirken 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun özellikle üç temel hükmüne dayanmıştır.

İlk olarak Kurul, sadakat kart sahibinin bilgisi ve rızası dışında üçüncü kişiler tarafından yapılan işlemlerin Kanun'un 5. maddesinde düzenlenen veri işleme şartlarından herhangi birine dayanmadığını değerlendirmiştir. Gerçekten de ilgili kişinin açık rızası bulunmadığı gibi, söz konusu veri işleme faaliyetinin sözleşmenin kurulması veya ifası için zorunlu olduğu da söylenemez.

İkinci olarak Kurul, bu uygulamanın Kanun'un 4. maddesinde yer alan genel ilkelerden "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil edebileceğini vurgulamıştır. Zira kart sahibi tarafından yapılmayan alışverişlere ilişkin verilerin ilgili kişi hesabına işlenmesi, veri kayıtlarının doğruluğunu ortadan kaldırmaktadır.

Son olarak Kurul, veri sorumlularının Kanun'un 12. maddesi uyarınca kişisel verilerin güvenliğini sağlamak için gerekli teknik ve idari tedbirleri alma yükümlülüğünü hatırlatmıştır. Sadakat kart üyelik sözleşmelerinde kartın üçüncü kişiler tarafından kullanılmaması yönünde hükümlerin bulunması, veri sorumlularının veri güvenliği yükümlülüğünü ortadan kaldırmamaktadır.

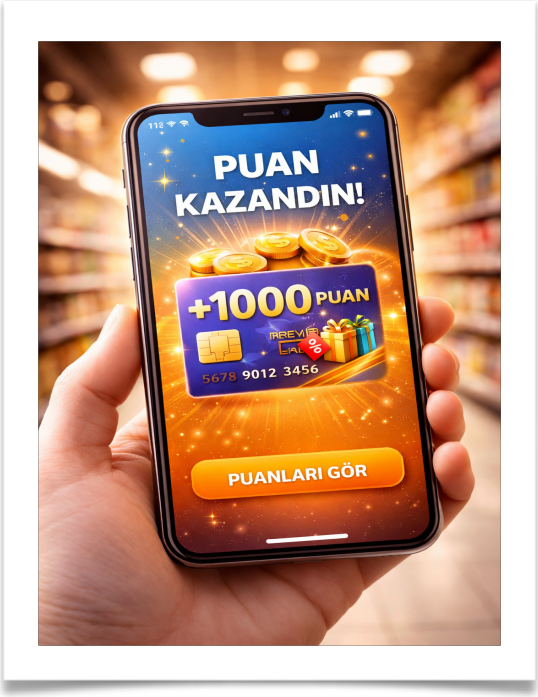
4. İlke Kararı ile Getirilen Yükümlülükler

Kurul tarafından alınan İlke Kararı ile sadakat kart sahibinin cep telefonu numarasının veya kart numarasının üçüncü kişiler tarafından alışveriş sırasında kasa görevlisine bildirilmesi suretiyle doğrulama yapılmaksızın işlem gerçekleştirilmesine imkan tanıyan uygulamaların sonlandırılması gerektiği belirtilmiştir.

Bu kapsamda veri sorumlularına sadakat kart işlemlerinin ilgili kişinin bilgisi ve onayı dahilinde gerçekleştiğini doğrulayacak teknik ve idari mekanizmalar kurma yükümlülüğü getirilmiştir. Bu doğrulama mekanizmaları; SMS yoluyla gönderilen tek kullanımlık doğrulama kodu, mobil uygulama üzerinden QR veya barkod okutma, fiziki sadakat kartın kasada ibrazı, sadakat kart şifresinin kasada işlem cihazına girilmesi,mobil bildirim onayı gibi yöntemleri içerebilecektir.

Kurul ayrıca doğrulama mekanizmalarının oluşturulmasında kullanıcıların yaş, eğitim düzeyi, ekonomik durum ve teknoloji okuryazarlığı gibi faktörlerin dikkate alınabileceğini ve farklı kullanıcı gruplarına yönelik alternatif doğrulama yöntemleri geliştirilebileceğini belirtmiştir.

Kararın önemli bir diğer yönü ise veri sorumlularına 6 aylık uyum süresi tanınmış olmasıdır. Resmî Gazete'de yayımlanma tarihinden itibaren başlayacak bu süre sonunda gerekli önlemleri almayan veri sorumluları hakkında Kanun'un 18. maddesi kapsamında idari yaptırım uygulanabilecektir.



5. Kararın Uygulamaya Etkileri

Söz konusu İlke Kararı, perakende sektöründe yaygın olarak kullanılan sadakat kart sistemleri açısından önemli bir dönüşüm gerektirmektedir. Özellikle yalnızca telefon numarasının sözlü olarak bildirilmesi suretiyle işlem yapılmasına dayanan mevcut uygulamaların büyük ölçüde değiştirilmesi gerekecektir.

Bu kararın uygulamada üç temel sonuç doğurması beklenmektedir. İlk olarak, sadakat kart işlemlerinde kimlik doğrulama mekanizmalarının standart hale gelmesi söz konusu olacaktır. İkinci olarak, veri sorumluları veri güvenliği risklerini azaltacak teknik altyapı yatırımlarına yönelmek durumunda kalacaktır. Üçüncü olarak ise tüketicilerin kişisel veri güvenliğinin güçlendirilmesi ve alışveriş verilerinin doğruluğunun sağlanması mümkün olacaktır.

Öte yandan kararın özellikle küçük ölçekli işletmeler açısından bazı operasyonel zorluklar doğurabileceği de göz ardı edilmemelidir. Bu nedenle doğrulama mekanizmalarının kullanıcı dostu ve pratik çözümler içerecek şekilde tasarlanması önem taşımaktadır.

6. Sonuç

Sadakat kart programları, işletmeler açısından müşteri sadakatini artıran ve veri temelli pazarlama faaliyetlerine imkan sağlayan önemli araçlar olmakla birlikte, bu sistemler kapsamlı kişisel veri işleme faaliyetlerini de beraberinde getirmektedir. Kişisel Verileri Koruma Kurulu tarafından alınan 11.02.2026 tarihli İlke Kararı, sadakat kart uygulamalarında kimlik doğrulama eksikliğinden kaynaklanan veri güvenliği risklerine dikkat çekmekte ve veri sorumlularına gerekli teknik ve idari önlemleri alma yükümlülüğünü hatırlatmaktadır.

Karar, özellikle kişisel verilerin doğruluğu ve veri güvenliği ilkeleri bakımından önemli bir hatırlatma niteliği taşımakta ve sadakat kart sistemlerinin kişisel verilerin korunması mevzuatıyla uyumlu hale getirilmesini hedeflemektedir. Bu yönüyle söz konusu İlke Kararı'nın, veri koruma hukukunun perakende, gıda, kozmetik, teknoloji, giyim gibi sektörlerin uygulamalarına yön veren önemli düzenleyici adımlardan biri olduğu söylenebilir.

KAYNAKÇA:

- https://www.kvkk.gov.tr/Icerik/8670/sadakat-kart-uyeligi-bulunan-bir-kisinin-cep-telefonu-numarasinin-veya-sadakat-kart-numarasinin-ucuncu-bir-kisi-tarafindan-alisveris-esnasinda-kullanilmasi-hakkinda-ilke-karari

EPSTEIN DAVASI İFŞALARINDA DİJİTAL ADLİ BİLİŞİMİN ROLÜ

AV.OĞUZHAN SEYMEN

Epstein davası gerek on yıllar öncesi gerekse 2025 yılı Aralık ayında FBI dijital data analizlerinin yayınlanması sonucu, *çocukların tecavüze-fiziki şiddete hatta cinayete ve organ trafiğine konu edilmelerine ilişkin semptom bir skandal* olmuştur.

İlgili gündemde; Dünya'nın vicdanında derin bir yara açıldığı gibi, saldırganların adlarının sansürlü olduğu, kurbanların adlarının ise açık olduğu , dosyaların çoğunun da hala kilit altında olduğu ve *kapitalist - ataerkil düzenin tüm hukuki-ahlaki normları nasıl da askıya aldığı* açıkça görülmüştür. [1]

"İfşalardaki dijital adli bilişimin rolüne[Digital Forensics]" giriş yapılması öncesinde de vurgulamak gerekir ki **işbu yazının kaleme alınma amacı; Türkiye'de üzülerek Epstein gibi bir gündem ortaya çıksaydı fail kimliklerinin hangi yöntemlerle tespit edilebileceğine, delillerin nasıl toplanılıp tartışılacağına ilişkin tavsiye ve emsal teşkil etmesidir.**

Nitekim Türkiye Cumhuriyeti'nin hukuk devleti sıralamasının neresinde olduğuna bakıldığında dileriz ki yazımız, *Epstein davasından esinlenilerek soruşturma ve kovuşturma makamlarına-bilirkişilere bilinçli hareket etmeleri ve adaletin vaktinde tecelli etmesi noktasında yangına su taşıyan karınca misali katkı sunabilsin.*

1- Dijital deliller kırılgandır. Delil vasfını yitirmeden bu delillerde makamlar, dijital parmak izlerinin toplanması sanatlarını konuşturmalıdır.

Bilgisayarlarda, cep telefonlarında, sunucularda ve ağ trafiklerindeki veriler; suçların aydınlatılması ve uyuşmazlığın çözümü için, toplanması, korunması, incelenmesi ve raporlanması sürecine Dijital Adli Bilişim, diyoruz. Bu kavram ile fakülte sıralarında **Bilgisayarlarda, Bilgisayar Programlarında Arama-Kopyalama-ve El Koyma** başlığı ile CMK m.134 bilgisi ile tanışmıştık.

Yargıtay Ceza Gene Kurul Kararlarında, Baroların iç yayınlarında ve Türkiye Barolar Birliği yayınlarında da bu bilgiye en çok; can alıcı kavramlar olan **"Hash Değeri[dijital imza], İmaj Alma Zorunluluğu[prijinal cihaz yerine bire bir kopya alınması]"** kavramları ile delillerin tartışılması noktasında rastlıyoruz.[2]

2- Tespitin doğru teknik ile yapılıp yapılmadığı; anayasal olarak, adil yargılanma hakkı, masumiyet karinesi [özellikle adli kolluğun şüpheliye suçlu muamelesi yapmasının önlenmesi] adına dikkatle incelenmelidir.

Delillerin toplanmasında, Zincirleme Veri Güvenliğinin ayakta tutulması

[Chain of Custody] masumiyet karinesi bakımından mühimdir.

Sözgelimi *bir hard diskin imajı alınırken hash değeri tutanağa geçirilmemiş ise iddia makamı "bu verilerin sonradan yüklenmediğini, önceden var olduğunu" tespit etmek* durumundadır. Böylesi bir şüphe varsa "o delil sanık aleyhine kullanılamayacağından" , "şüpheden sanık yararlanır."

3- Türkiye'de bir fail kimliği, şifreli ağların deşifre yöntemiyle-şifre kırma yöntemleriyle-Europol/Interpol işbirliğiyle ve şahsın nihayet deşifre edilmesi sonucu güvenle tespit edilebilmektedir:

Kurtlar Vadisi ve Ezel isimli dizilerde, Epstein davasını akıllara getiren bazı sahneler vardır.[3.]

Ezel dizi sahnesinde Epstein'e; dünyanın en iyi sanatçılarının, sporcularının, dilediğini kuralsızca yapabildiği eğlence mekanı adı altında Epstein'in aldatıcı şatafatı karşısında nasıl manipüle edildikleri gösterilmiştir.[3.a.]

Kurtlar Vadisi dizi sahnesinde de Yüce Majeste ve Artur karakterleri gibi karanlık odakların, özel şifreli telefon ağları ile haberleştiğini görüyoruz.[3.b.]

Üzülerek rastlıyoruz ki bilişim suçlarına meraklı olan **Bay Mükerrirler**, soruşturma evrelerinde avukatlarına yakalanmayacaklarından emin konuşurlar. Şimdilik kendilerine bu güveni ***"Uçtan Uca Şifreleme" (E2EE)*** özellikli yeni nesil aplikasyonlar vermekte. Hatta fail yine hiç yakalanmayacağı yönünde şöyle düşünüyor: *"Veri sadece kendi cihazımda ve cihazımı, kendini imha moduna aldım, veriye ulaşmanız imkansız."* Bay Mükerrir'i, akıl almaz sandığı bu şeytanlığından tebrik ederiz ama **lades…** Çünkü hem mükerririn bu yakalanmayacağına olan güveni hem de aşağıdaki delillerin toplanması süreçleri, bazı dizi repliklerini anımsatıyor: *'Senden büyük konsey varsa, konseyden büyük devlet var.' Büyük balık, küçük balığı yer.* Büyük balık, istihbarat teşkilatı ile kurumdur. Teşkilat ve Kurum, ilgili failin;

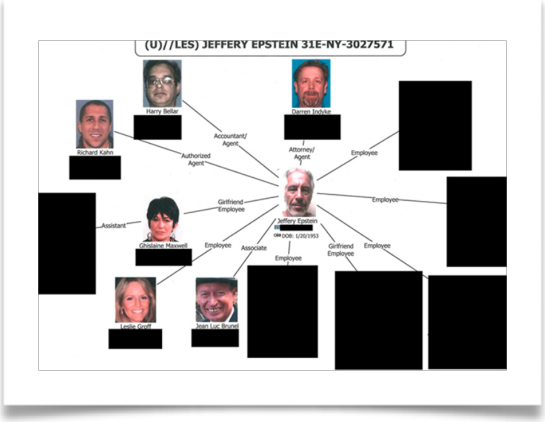
3.1) a) Şifreli Ağların Deşifre Yöntemi olan; SkyECC, EncroChat veya Anom gibi "kırılamaz" denilen özel şifreli telefon ağları inceleniyor.

b) Şifre Kırma (Decrytion) yöntemlerinden, Chip-Off, Brute Force [Cellebrite, GrayKey vb. özel donanımlarla) ve RAM Analizi yapılıyor.

c) Europol/Interpol işbirliği ile veriler, direkt kaynağından-uluslararası resmi yoldan geliyor.[4]

d) Şifreli ağlarda da Blokzincir üzerinden yapılan para trafiği izlenmesi neticesinde (Blockchain Chainalysis ile) kıskıvrak yakalanıyor.

3.2) Fail nasıl deşifre ediliyor? MİT ve Emniyet Müdürlüğü, belirtilen şifreli ağları kullanıp hedef kişiyi takip ederek tespit ediyor. Suç mahalline operasyon yürütüyor, suça ilişkin hücreyi açıksa suçüstü yakalatabiliyor ve nihayetinde suç eşyası olan cihazı ele geçiriyor. Dijital imza diye belirttiğimiz Hash Değeri ile İmaj Alıyor, orijinali üzerinden bir kopya oluşturuyor. Faili de; yukarıda belirtilen şifre kırma yöntemleri ile veya bulut sisteminden gelen verilerle eşleştirerek deşifre ediyor.



Fezleke de bu deşifre doğrultusunda günlük "log" kayıtları(zaman damgası-kullanıcı adı-IP adresi-girişin yapılıp yapılmadığı-dosyanın silinip silinmediği) bilgisi, mesaj kayıtları ve konum verilerine ilişkin HTS kayıtları ile raporluyor.

4- "Epstein Davasında" hangi olayların geliştiğini ve aktörlerinin nasıl bulunduğunu da; yazımızın esin kaynağı olduğundan belirtmekte yarar vardır.

4.a) Epistein davasının iddia ve savunma makamlarını *esas mağdur; Virginia Giuffre, sanık; Prens Andrew* (Birleşik Krallık'ın kraliyet ailesi üyesidir) ve *suç örgütünün yöneticileri J. Epstein ile bayan G. Maxwell* oluşturuyor. Delilleri 2025 Metadata Raporları ile tartıştıran da *FBI'dır*.[5]

4.b) Delillerin nasıl tartışıldığına en son bağlanacak olan, Epstein sürecinin gündemde en çok konuşulan kısmı da şöyledir:

4.b.1) İddiaya göre bir Londra buluşması var ve meşhur 2001 tarihli bir "belden sarılma" fotoğrafı çekilmiş. Bu foto , Prens'in ta 2019'da savunmasına konu oluyor.

Fotoğraf 2025'te tüm dünya gündemine oturarak orijinali ile taranmış hali mahkemeye meta-data olarak sunuluyor.

Prens 2026'da Lindra'da tutuklanıp ifadeye getiriliyor. Mağdure V. Giuffre, Epstein ve Maxwell'in failliğinde Prens ile Londra, New York ve Virgin Adaları'nda zorla birlikte olduğunu iddia ediyor.

Savunmasında Prens ise Giuffre ile hiç tanışmadığını, fotoğrafın da sahte olduğunu iddia ediyor.

Delil incelemesine ilişkin **orijinal foto analizinde** FBI, fotoğrafın arka planındaki ışık kırılmalarını ve gölge piksellerini inceliyor ve fotoğrafın montaj olmadığını , 2001'in kimyasal baskı özelliklerini taşıdığını doğruluyor.

Epstein'ın **uçağındaki dijital kayıtla**r da Prens'in iddia edilen tarihlerde mağdurun bulunduğu lokasyonlar olan Londra-New York hattında olduğunu da doğruluyor.

Şayet sanık lehine yorumlanabilecek iki ihtimal de vardır: veriler silinmiş olabileceği ve kabul gördüğü takdirde sanık tanığının anlatımlarıdır. Çünkü Prens'in özel ofisindeki 2001-2002 dijital yazışmalarda **"sunucu temizliği"** yapılmış.

Bazı e-maillerin Hotmail/AOL(eski amerikanın e-posta altyapısı) üzerinden gelmesi de delillere, sanık aleyhine dışarıdan müdahale edilip edilmediği şüphesi uyandırıyor.

Ayrıca mağdure, şikayetinde olay günü Prens'in terli olduğunu iddia ederken Prens ise Falkland Savaşı'ndaki bir tıbbi durum nedeniyle terleyemediği yönünde kendini savunuyor. Bununla birlikte sanık Prens'in terleyememe iddiası, dijital arşivden alınan, 2000'li yılların başındaki gece kulübü fotosu ile teknik anlamda açıkça çelişiyor.

Öte yandan suça konu fotonun çekildiği sanık bayan Maxwell'in evinin,

o güne ait kamera kayıtlarının kayıp olması şüphesinden de sanık yararlanabilir.

4.b.2) Tüm bu gündeme göre burada delillerin , yazımızın 3.1) ve 3.2.) kısımlarına göre toplanıp tartışıldığına atıf yapmakla yetiniyoruz.

5- Nihayet Epstein davasının Türkiye gündemine girmesinin önemine de değinelim.

Epstein davası kapsamında mühürsüzleşen (soruşturma gizli olmaktan çıkıp aleni hale geldiği) 1328 numaralı dosya hazırlanıyor ve eklerinde dijital kayıtlar tutuluyor.

Süreç , taciz şebekesi ile ilişkilendirilen Pilot N. Marçinko'nun ifadeleri ve dosyadaki Avukat Ezell'in tespitleri üzerinden şekilleniyor.

Sanığın "susma hakkı" bir suçlamaya bir engel oluşturmak ile birlikte yukarıda belirtilen uçuş kayıtları ve iletişim log'ları gibi dijital verilerin doğrulanması kritik bir eşik teşkil ediyor.

Bununla birlikte listede yer alan tam bir kamu malı niteliği taşıyan ünlü isimlerin verileri, elbette kesin delil oluşturmuyor.

Bu tür delillerin **"sadece bir temas verisi"** olarak kabul edilmesi gerekmekle birlikte , temas verisi olmasının; veri madenciliği süreçlerinde bağlam dışı yorumlanmaması gerektiği, vurgulanıyor.

Bunun en büyük nedeni de ilgili kayıtların, **1999 depremi sonrası Türkiye'den çocuk kaçırıldığına dair iddiaları** içermesi. Bu bakımdan da **"delil zincirinin bütünlüğüne"** önem atfediliyor.

KAYNAKÇA:

[1] Cumhuriyet gazetesi, 05.02.2026, Ergin Yıldızoğlu'nun köşe yazısı, s.9

[2] Google Scholar ; "Cyber forensics in high-profile sex trafficking cases

[3] Kurtlar Vadisi ve Ezel dizi sahneleri:
3.a) https://www.youtube.com/watch?v=vRL_wE1Bwpc

3.b) https://www.instagram.com/reel/DUgQJhmjJDS/

[4] New York Güney Bölge Mahkemesi (SDNY) PACER sistemindeki mühürsüzleşen dijital delil listelerine ilişkin resmi kararlar

[5] LexisNexis veya Westlaw ; "Epstein digital discovery

[6] Derlemenin bel kemiği diğer web adresleri

6.a. www.economictimes.indiatimes.com

6.b. www.ohchr.org

6.c. www.britannica.com

6.d. www.time.com

6.e. www.justice.gov

6.f. www.doğrulukpayı.com

DİJİTAL OYUN İÇİ SATIN ALIMLARA HUKUKİ BİR BAKIŞ

AV. İREM NALBANT

Dijital oyun endüstrisi son yıllarda yalnızca teknolojik bir dönüşüm geçirmemiş, aynı zamanda ekonomik modelini de köklü biçimde yeniden yapılandırmıştır. Dijital oyun içi satın alımlar kapsamında birçok alt dal türemiş olup ciddi meblağlar konuşulur olmuştur.

Bu bağlamda ilk olarak "in-game purchases" yani "oyun içi satın alımlar" kavramı ele alınmalıdır. Bu kavram, oyuncuların oyun içerisinde gerçek para kullanarak dijital içerikler satın almasını ifade eder ve bu içerikler bazen yalnızca görsel değişiklikler sağlarken bazen de doğrudan oyun performansını etkileyebilir. Örneğin bir oyuncunun karakterine farklı bir görünüm kazandırması yalnızca estetik bir değişiklik yaratırken, karakterin saldırı gücünü artıran bir öğe satın alması doğrudan rekabet avantajı doğurur.

Oyun içi satın alımlar içerisinde en çok tartışılan yapılardan biri olan "Pay-to-Win (P2W)", Türkçeye "kazanmak için ödeme" şeklinde çevrilebilir. P2W temel haliyle, bir oyuncunun gerçek para harcayarak oyunda diğer oyunculara kıyasla somut bir avantaj elde etmesini ifade eder. Teknik anlamda bu avantaj karakter özelliklerinin artırılması, diğer oyuncuların ancak mesai ve çaba ile erişebileceği güçlü ekipmanlara anında erişim sağlanabilmesi veya oyun içi ilerlemenin hızlandırılması gibi mekaniklerle ortaya çıkar ve oyun içi rekabeti doğrudan etkiler.

Bu kavramın anlaşılabilmesi için onunla ilişkili diğer teknik terimlerin de açıklanması gerekir, zira pay-to-win mekanikleri çoğu zaman tek başına değil, daha geniş bir ekonomik sistemin parçası olarak ortaya çıkar.

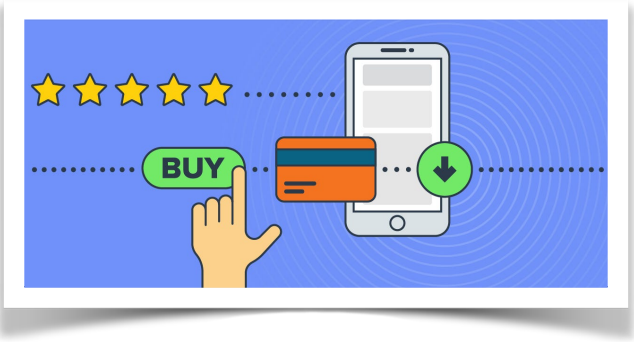
Pay-to-win tartışmalarının merkezinde yer alan bir diğer kavram "loot box", yani "rastgele ödül kutusu" sistemidir. Bu sistemde oyuncu belirli bir ücret karşılığında içeriği önceden bilinmeyen bir dijital kutu satın alır ve kutudan çıkacak ödül tamamen şansa bağlıdır. Teknik olarak bu mekanik, olasılık temelli bir ödül dağıtım algoritmasına dayanır ve çoğu zaman düşük ihtimalle yüksek değerli ödüller sunar. Basit bir anlatımla oyuncu bir kutu satın alır ve içinden ne çıkacağını bilmeden risk alır. Bu durum hukuki açıdan kumar benzeri yapı tartışmalarını gündeme getirmektedir, çünkü oyuncuya sunulan olasılıkların açıkça belirtilmemesi tüketicinin bilinçli karar verme yetisini zayıflatır. Türk hukukunda bu tür durumlar yanıltıcı ticari uygulama kapsamında değerlendirilebilir.

Ek olarak "pay-for-convenience", yani "kolaylık için ödeme" kavramı da pay-to-win tartışmalarının sınırlarını belirleyen önemli bir unsurdur. Bu kavram, oyuncunun doğrudan güç kazanmak yerine oyun içi ilerleme sürecini hızlandırmak amacıyla ödeme

yapmasını ifade eder. Teknik olarak bu sistem, deneyim puanı artışı, bekleme sürelerinin kaldırılması veya kaynak üretiminin hızlandırılması gibi mekaniklerle çalışır. Basit bir ifadeyle oyuncu saatler sürecek bir ilerlemeyi para ödeyerek dakikalar içinde tamamlayabilir. Her ne kadar bu sistem doğrudan rekabet avantajı sağlamıyor gibi görünse de dolaylı olarak oyuncunun daha hızlı güçlenmesine olanak tanıdığı için pay-to-win kapsamında değerlendirilip değerlendirilmeyeceği tartışmalıdır. Hukuki ihtilaf bu noktada genellikle oyunun tasarımının bilinçli olarak yavaşlatıldığı ve oyuncunun ödeme yapmaya zorlandığı iddiası üzerinden ortaya çıkar ve bu durum tüketicinin ekonomik davranışının manipüle edilmesi olarak değerlendirilebilir.

Bir diğer önemli mekanik olan "battle pass", yani "sezonluk içerik sistemi", oyunculara belirli bir süre boyunca ilerleme kaydederek ödüller kazanma imkânı sunar. Bu sistemde genellikle ücretsiz ve ücretli olmak üzere iki ayrı ödül hattı bulunur ve ücretli olan hat daha değerli içerikler sunar. Teknik olarak bu yapı, oyuncunun oyun içinde geçirdiği süreyi ve performansını ödüllendiren bir ilerleme sistemi olarak tasarlanmıştır. Ancak ücretli katmanın sunduğu ödüllerin oyun içi performansı etkilemesi halinde bu sistem de pay-to-win tartışmalarına dahil olur. Çünkü yalnızca ücretli kullanıcıların erişebildiği güçlü ekipmanların bulunması gibi durumlar rekabet dengesini bozabilir. Hukuki açıdan bu durum, tüketici üzerinde zaman baskısı yaratılması ve satın alma kararının bu baskı altında verilmesi açısından tartışılabilir.

Bu teknik ve kavramsal çerçeve içerisinde pay-to-win mekaniklerinin hukuki ihtilaflara yol açmasının temelinde çoğunlukla satın aldığı içeriğin beklenen/vadedilen faydayı sağlamaması, tüketicinin yanıltılması, yeterince bilgilendirilmemesi veya sözleşmesel dengenin bozulması yer alır. Özellikle bir oyunun pazarlama sürecinde "adil rekabet" veya "beceriye dayalı oyun" vurgusu yapılmasına rağmen gerçekte ödeme yapan oyunculara avantaj sağlanması, Türk hukukunda yanıltıcı ticari uygulama olarak değerlendirilebilir. Bu durumda tüketici, satın alma kararını hatalı bir algıya dayanarak vermiş olur ve bu durum hukuki sorumluluk doğurur. Bunun yanı sıra loot box gibi sistemlerde ödül olasılıklarının açıkça belirtilmemesi, bilgilendirme yükümlülüğünün ihlali olarak kabul edilebilir. Satın alınan içeriğin beklenen/vadedilen faydayı sağlamaması iddiası ise ayıplı hizmet kapsamında değerlendirilerek tüketici hakem heyetleri veya tüketici mahkemeleri önüne taşınabilir.



Sözleşmesel boyutta ise oyun şirketleri tarafından sunulan son kullanıcı lisans sözleşmeleri, genellikle oyun içi dengenin değiştirilebileceğini ve satın alınan içeriklerin mülkiyet oluşturmadığını düzenler. Ancak bu tür hükümler, Türk Borçlar Kanunu kapsamında genel işlem şartı olarak değerlendirilir ve tüketici aleyhine dengesiz bir durum yaratmaları halinde geçersiz sayılabilir. Bu nedenle bir oyuncunun ödeme yaparak elde ettiği avantajın sonradan ortadan

kaldırılması, sözleşmesel sorumluluk doğurabilir.

Tüm bu ihtilafların çözümünde Türk hukukunda farklı mekanizmalar devreye girer ve bu mekanizmalar somut olayın niteliğine göre değişiklik gösterir. Örneğin oyuncular ayıplı hizmet veya yanıltıcı ticari uygulama iddialarıyla tüketici hakem heyetlerine veya tüketici mahkemelerine başvurabilir. Yanıltıcı tanıtım ihbarları gibi reklam konularında idari yaptırımlar uygulanması açısından Reklam Kuruluna başvurulabilir. Özellikle çocuk oyuncuların hedef alındığı sistemlerde KVVK bağlamında sorumluluklar gündeme gelebilir. Bunun yanı sıra sözleşmesel uyuşmazlıklar genel mahkemelerde çözümlenir ve burada dürüstlük kuralı ile sözleşme dengesi temel değerlendirme ölçütleri olarak öne çıkar.

Dijital oyunların giderek daha karmaşık ekonomik sistemler haline gelmesi, mevcut hukuki düzenlemelerin yorum yoluyla genişletilmesini zorunlu kılmaktadır. Türk hukukunda henüz bu alana özgü özel bir düzenleme bulunmamakla birlikte, mevcut tüketici hukuku, sözleşme hukuku ve veri koruma rejimi, pay-to-win tartışmalarından doğan uyuşmazlıkları çözmek için yeterli bir temel sunmaktadır.

Yine de, teknolojik gelişmelerin hızı ve bu alandaki ekonomik potansiyel dikkate alındığında, 2026 yılı içerisinde mecliste konuşulmaya başlanan e-oyun yasası ile birlikte konuya ilişkin özel bir yasa ve içtihadın oluşması beklenmektedir.

YAPAY ZEKÂ KULLANAN AVUKATLAR İÇİN VERİ KORUMA REHBERİ*

AV. ZEYNEP HESAPDAR ARTUN

GİRİŞ

Hukukun, insan hayatının merkezine yerleşen tüm yenilikleri yakından takip etme zorunluluğu son yıllarda özellikle teknolojik gelişmelerle beraber daha fazla karşımıza çıkmaktadır. Uyuşmazlık çözümü konusunda çağa uygun kararlar alınabilmesi ve hatta önleyici hukukun da ihtiyaçları gerçek anlamda karşılaması açısından teknolojik gelişmelere uygun hukuki adımlar atılması gerektiği şüphesizdir.

Teknolojinin dönüm noktası olarak adlandırabileceğimiz yapay zekâ da hayatımıza girdiği günden itibaren pek çok hukuki tartışmayı gündeme getirmiş; yeni ihtiyaçlar, uyuşmazlıklar ve gelişmelere kapı açmıştır.

Yalnızca yapay zekânın işleyebileceği suçlar, yapay zekâ ile yazılan dilekçe veya sözleşmeler gibi konuların tartışılması değil, yapay zekânın kullanımı konusunda da hukuki açıdan koruma ve dikkat gerektiren pek çok husus bulunmaktadır. Yapay zekâ, hızlı gelişimiyle; tüm sektörlerin, idarelerin, yönetimlerin başlıca kaynaklarından biri haline gelmeye başlamış ve çoğunlukla akla ilk gelen araç olma noktasına erişmiştir. Pek çok yapay zekâ aracı da çeşitli amaçlara hizmet etmek için üretilmiş ve hayatımızın merkezinde yerini almış haldedir.

Veri güvenliği ise yapay zekânın bu hızlı gelişiminden olumsuz etkilenmiştir. Veri korumanın önemi özellikle kişilerin bilgileri ve özel hayatlarına hâkim olunan meslek grupları açısından büyük önem taşımakta ve birtakım yükümlülükleri de beraberinde getirmektedir. Ne yazık ki çoğu zaman yapay zekâ kullanımında veri gizliliğinin önemi kullanıcılar tarafından dikkate alınmamakta ve sürekli olarak veri ihlali yapılmaktadır.

Yapay zekâ araçlarının çeşitli amaçlara yönelik olarak özel niteliklerle donatılması, hukuk alanında da özellikle avukatlık mesleğinde her gün bir başka yenilikle karşımıza çıkmaktadır.

Yapay zekâ, biz avukatların mesleki süreçlerinde, yerimizi alacak bir yenilik değil; aksine süreci çağa uygun ve ihtiyaçlara verimli şekilde karşılık verebilmemiz için kullanabileceğimiz araçlardan yalnızca biridir. Yapay zekâ, mesleğimize yönelik üretilen araçlarıyla tehdit unsuru olarak algılansa da esas tehlike, yapay zekâyı veri ihlali yaparak kullanmaktadır.

Mesleki faaliyetlerimize devam ederken gerek profesyonel gerekse sosyal yaşamda kullandığımız yapay zekâ araçlarında veri güvenliğine gereken dikkati verdiğimizde; zaman yönetimi, analiz gücü veya kişisel verilerin korunması hakkında daha güvenilir ve sürdürülebilir bir danışmanlık sunmamız mümkündür.

---

* Bu makalede kullanılan görseller, anlatılan tüm tedbirler alınarak yapay zekâ araçları tarafından üretilmiştir.

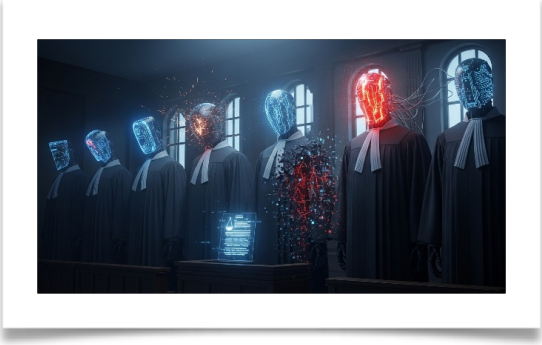
Bu makalenin devamında, avukatların yapay zekâyı kullanırken veri güvenliğini sağlayabilmesi açısından önemli noktalara değinilecek, özellikle kişisel verilerin korunması noktasındaki risklere yer verilerek bunlara ilişkin öneriler sunulacaktır.

KVKK VE YAPAY ZEKÂ VERİ İŞLEME

6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu kanunda yapılan değişiklikler, önleyici hukukun önemini veri korunması hakkında ortaya koymaktadır. Zira bu kanun ile kişisel verilerin korunmasına yönelik mevzuatımız, birtakım ilkeler ile beraber özellikle hesap verilebilirlik ve şeffaflık gibi ilkelerin yapay zekâ gibi teknolojinin yeniliklerine uyum konusunda önemli önleyici düzenlemelere yer vermektedir. Veri koruması alanındaki titiz çalışma ve düzenlemeleri yalnızca bir kurallar listesi olarak görmek, gerçek bir veri koruması sağlamayacaktır. Böyle bir yaklaşım eksik olup, örneğin VERBİS'e kayıt konusundaki istisnalar gibi hususlarda açık bir veri ihlaline yol açabilecektir.

Özellikle biz avukatların, yaptığımız işin doğası gereği müvekkil veya danışanların kişisel bilgi ve verilerine hâkim olmamız, yapay zekâ araçlarının dikkatsiz kullanılması ile büyük veri ihlalleri, etik sorunlar ve mesleki sorumluluk gibi sonuçlarla karşılaşmamıza neden olabilecektir.

KVKK'nın 6.maddesinde özel nitelikli kişisel verilere yer verilmiştir. Özellikle bu gruba giren kişisel veriler kanunda belirtildiği üzere ancak zorunlu ve gerekli durumlarda işlenebilmektedir. Yapay zekâ araçları mesleki faaliyetler nedeniyle kullanılırken çoğunlukla belge özeti, dilekçe hazırlığı aşamasında yardım alma, somut olayı paylaşarak hızlı mevzuat taraması, içtihat araştırması gibi talepler yapay zekâ yazılımlarına sunulmaktadır. Meslek faaliyetlerimiz gereği kimi zaman KVKK'da özel nitelikli olarak sayılan kişisel verilerin yer aldığı pek çok bilgi ve belgeye erişebilmekteyiz. Bu gibi belgelerin doğrudan yapay zekaya sunulması açık bir veri ihlali doğurmaktadır. Zira bu veriler hakkında yapay zekâ araçları aracılığıyla yapılacak herhangi bir işlem, veri işlemesi anlamına gelmektedir ki bu durum da kanunun 6.maddesinde belirtilen zorunluluk veya gereklilik hallerini çoğu zaman karşılamamaktadır.



Bununla beraber, yapay zekâ araçlarıyla paylaşılmak suretiyle işlenmesi halinde veri ihlali doğuracak olan veriler yalnızca 6.maddede yer alan özel nitelikli kişisel veriler değildir. KVKK, 3/1-d maddesi kişisel veri kavramını *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlamaktadır. O halde bir verinin kişisel veri sayılabilmesi için o verinin doğrudan kime ait olduğunu içermesi gerekmemektedir. Herhangi bir verinin kime ait olduğu belirtilmeden bunun anlaşılabilir şekilde sunulması dahi bu verinin kişisel veri olduğunun kanun tarafından kabul edildiğini göstermektedir.

Kanun, her ne kadar özel nitelikli kişisel veri ihlallerini çok daha ağır yaptırımlara bağlasa da bunlar dışında kalan fakat kanun kapsamında kişisel veri olarak sayılabilecek her türlü verinin, kanunda yer verilen koşullara

uygun olmadan yapay zekâ araçları ile paylaşılması kişisel veri ihlali anlamına gelmektedir.

Yapay zekâ araçlarının tümü, esasında bir yazılım ürünü olduğundan tümünün bir kaynağı bulunmaktadır. Dolayısıyla bu yapay zekâ araçlarının, büyük veri kümeleri içerisinde yer alan bilgileri işleyerek ürettiği yeni bilgiler de bu veri havuzunda yer almakta ve hiçbir zaman kaybolmamaktadır. Bu sebeple hangi yapay zekâ aracı olursa olsun, paylaşılan bilgilerin tümü de bu veri havuzuna gireceğinden paylaşılan bilgi ve belgelerde kişisel veri yer alması doğrudan bir veri işlemesi anlamına gelecektir.

Yapay zekâ araçlarının güncelliğini koruyarak hayatımızda daha da gelişerek var olmaya devam etmesinin tek yolu da aslında bu veri havuzlarının sürekli büyüyüp derinleşerek daha fazla veri depolamasından geçmektedir. Yapay zekânın neredeyse tüm meslek dallarında, sosyal hayatın içinde ve hatta kamu kurumlarında yapılan işlemlerde büyük rol oynaması; esasen pek çok bilgiyi aynı anda, istenilen odak noktasında toplayabilecek, bunları değerlendirerek yeni bir bilgi ve hatta kimi zaman görüş ortaya koyabilecek şekilde tasarlandığından büyük bir zaman tasarrufu gibi görünmesidir. Tam da bu sebepten yapay zekâ her zaman çok daha fazla veriye ve hatta kişisel veriye ihtiyaç duyacaktır. Aksi halde kaynağı sınırlı kalacak ve böylesi bir yazılım ürününden beklenilen performansı tam olarak sergileyemeyecek noktaya gelecektir. Bu nedenle günlük hayatta bu araçları kullanırken çoğunlukla önemsiz gibi görünen birtakım veriler, aslında yapay zekânın en çok ihtiyaç duyduğu kaynaktır.

Sentetik veri kavramı, bu hususu çok daha kolay anlamamıza, kişisel verinin yapay zekâ araçları nezdinde sandığımızdan çok daha büyük bir yeri olduğunu kavramamıza yardımcı olacaktır. Yapay zekâ araçlarının, gerçek verileri değerlendirerek bunların yapısı ve istatistiksel özelliklerine göre bir sonuç çıkartıp bu yönleriyle gerçek veriyi taklit ederek oluşturulan yeni veriler; sentetik verilerdir. Sentetik veriler, çeşitli alanlarda farklı amaçlara hizmet etmek için üretilse de yapay zekânın öğrenmesine ve üretiminin devam etmesine katkı sunmak amacıyla da üretilmektedir. Yalnızca bu kavram dahi, yapay zekânın sürekli olarak yeni verilere ihtiyaç duyduğunun bir göstergesidir. Üstelik, yapay zekânın pek çok kişi ve meslek grubu tarafından henüz tam olarak kavranamamış olduğu bu dönemde, yapay zekâ araçlarıyla pek çok kişisel verinin de bilinçsizce paylaşıldığı bir dönemde dahi sentetik verilerin üretilmesine de ihtiyaç duyulmaktadır. Yapay zekâ araçlarında kişisel verilerin paylaşılmaması gerektiği hakkında yeterli bilgi ve bilincin olmadığı bir dönemde dahi yapay zekâ araçlarının geliştirilmesi için sentetik verilere de ihtiyaç duyulması, yapay zekâ araçlarındaki veri açlığını net şekilde ortaya koymaktadır.

Özellikle biz avukatlar gibi işimizin niteliği gereği, özel nitelikli kişisel veriler dahil olmak üzere pek çok kişisel veriye ulaşılması mümkün olan meslek gruplarında, bu farkındalık çok daha erken oluşmalı, tedbirler çok daha erken şekilde hayatlarımıza ve bürolarımıza entegre edilmelidir.

RİSKLER VE TEHDİTLER

Yapay zekâ araçlarının veri açlığının oluşturduğu riskler özellikle kişisel veriler anlamında çok daha fazla karşımıza çıksa da tüm riskleri yalnızca bu alanla sınırlamamız mümkün değildir. Her ne kadar buraya kadar yalnızca yerel mevzuatımıza yer verilmiş olsa da yapay zekâ araçları ile kolaylaşan ve

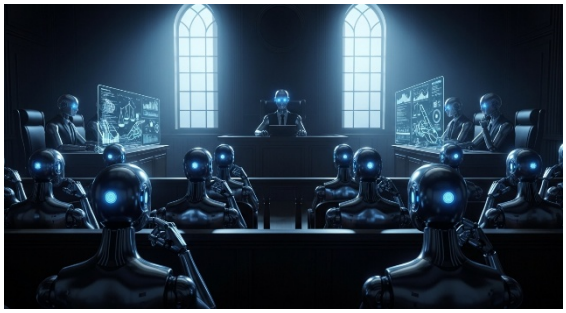
yaygınlaşan kişisel veri ihlali, ulusal alanda olduğu gibi uluslararası alanda da önem taşımakta ve risk barındırmaktadır. Bu konu toplum ve ülke güvenliği, kişi ve toplum menfaatleri ve zaafları gibi pek çok açıdan değerlendirilebilecek olup kişisel veri paylaşımına dikkat edilmeden ve önlem alınmadan bu araçların kullanılmaya devam etmesi, güvenlik zafiyeti oluşturacaktır.

Yapay zekâ araçlarının kişisel veri hukuku dışında; siber güvenlik, fikri mülkiyet, tüzel kişilerin know-how ve gizli bilgileri, kamu kurum ve kuruluşlarının barındırdığı kişisel veri dışındaki tüm diğer bilgiler, yanlış bilginin yayılması, ulaşılması ve ihlali kolaylaşan bilgiler ile ekonomik zafiyetlerin ortaya çıkması veya kolaylaşması, bir suçun faili veya mağduru olmakla beraber hukuk mahkemeleri önünde bir tazminat yükümlülüğü ile insan hakları ihlali gibi çok fazla farklı alanda da risk barındırmaktadır.

Yapay zekâ araçlarının bilinçsiz kullanımının birbirinden bağımsız ve çok sayıda alanın ihlalini oluşturacağı gibi; bu makale kapsamında özellikle değinilmesi gereken, biz avukatların yapay zekâ kullanımının bizim için ne gibi riskleri beraberinde getirdiğidir.

Bu riskleri anlayabilmek için öncelikle yapay zekânın avukatlar tarafından, mesleki faaliyetleri kapsamında hangi amaçlarla kullanılmakta olduğunun özetlenmesi gerekir. Genellikle zaman tasarrufu açısından belge özetleme, mevzuat taraması, içtihat araştırmayı kolaylaştırmak ve ne yazık ki kimi zaman da dilekçe oluşturmak için yapay zekâ araçlarının avukatlar tarafından kullanıldığı görülmektedir. Dolayısıyla bu şekilde bir kullanımda ihlal edilmesi en kolay ve en çok karşımıza çıkan alan kişisel veri hukukudur.

İzah edildiği üzere, yapay zekâ araçlarının en büyük kaynağı yeni verilerdir. Avukatların bu araçlarla paylaştığı kişisel veriler de yapay zekanın bu kaynağını doğrudan sağlarken kişisel veri ihlali doğurmaktadır. Fakat bir avukat açısından risk yalnızca kişisel veri ihlali değil; aynı zamanda sır saklama yükümlülüğünün de ihlali anlamına gelmektedir.



1136 sayılı Avukatlık Kanunu 34.maddesinde *"Avukatlar, yüklendikleri görevleri bu görevin kutsallığına yakışır bir şekilde özen, doğruluk ve onur içinde yerine getirmek ve avukatlık unvanının gerektirdiği saygı ve güvene uygun biçimde davranmak ve Türkiye Barolar Birliğince belirlenen meslek kurallarına uymakla yükümlüdürler."* demek suretiyle avukatların özen yükümlülüğü vurgulanmaktadır. Yapay zekâ araçlarının ortak ve genel özelliği, topladığı ve erişebildiği bilgi ve verileri birleştirerek bir sonuç ortaya koymasıdır. Ortaya koyulan bu sonuç, kimi zaman yeni ve uydurma bir senaryo üretilmesi olarak da karşımıza çıkmaktadır. Örneğin pek çok avukat, yapay zekânın hayatımıza girmesiyle, çok büyük zaman tasarrufu olacağı ümidiyle yapay zekâ ile emsal karar, içtihat arama yoluna başvurmuş; sonuçlarında da yapay zekâ araçlarının kendilerinin bir karar ürettiğini görmüşlerdir. Dolayısıyla yapay zekâ araçlarının çıktılarının her zaman doğru veya gerçek olduğu söylenemez. Yine aynı örnek üzerinden

devam edecek olursak; böylesi bir uydurma yargı kararına dilekçelerde yer vermek, mevcut dosya açısından olumsuz sonuçlanabileceği gibi açıkça avukatın özen yükümlülüğü ihlalidir. Zira bu kararların doğruluğunun kontrol edilmeden doğrudan kullanılma yoluna başvurulması, meslek kurallarına aykırı olacaktır.

Bu 34.maddeye paralel olarak; Türkiye Barolar Birliği Meslek Kuralları ve 6098 sayılı TBK'nın vekalet sözleşmelerinde hesap verme yükümlülüğünü düzenleyen 508.maddesi de avukatların mesleki yükümlülükleri altında müvekkillerine hesap verme yükümlülüğü olduğunu da göstermektedir. Bu yükümlülük esasında müvekkili aydınlatma, bilgi verme anlamına da geldiğinden yapay zekâ araçlarının ilgili müvekkilin işleri çerçevesinde kullanıldığı ve sonuçları ile ilgili olarak bilgi verilmesi de avukatlık mesleğinin yükümlülükleri arasındadır. Müvekkilin bilgileri arasında çok fazla kişisel veri de bulunacağından KVKK kapsamında kişisel verilerin anonimleştirilmesi gibi yöntemlere başvurulmuyorsa veya başvuruluyorsa ne gibi bir yöntemle verilerinin yapay zeka araçlarıyla paylaşıldığı gibi bilgilerin de müvekkile veriliyor olması, hesap verme yükümlülüğü kapsamındadır.

Yine aynı kanun, 36.maddesi ile "*Avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve barolar organlarındaki görevleri dolayısiyle öğrendikleri hususları açığa vurmaları yasaktır.*" şeklinde, avukatların sır saklama yükümlülüğünü düzenlemektedir. Maddeden, avukatların sır saklama yükümlülüklerinin yalnızca kişisel bilgilere ilişkin olmayıp öğrenilen her türlü hususu kapsadığı açıkça anlaşılmaktadır. Yukarıda anlatıldığı üzere, yapay zekâ araçlarının veri havuzları, işlenmek üzere bilgi topladığından bizlerin paylaştığı her türlü bilgi de esasında bu veri havuzunu beslemek üzere sunulan ve mutlaka işlenecek olan verilerdir. Dolayısıyla bizlerin de yapay zekâ ile paylaşılan tüm bilgi ve belgeler, maddede belirtilen açığa vurmak işlemini karşılamaktadır.

Ülkemizde yargıda yapay zekâ çalışmaları veya hedefleri veya yalnızca avukatlara yönelik piyasaya sürülen yapay zekâ araçları mevcut olsa da; mevzuatımız bu araçları resmi olarak tanımamaktadır. Fakat bununla beraber, bu araçların kullanılması, bunlardan çeşitli yöntemlerle faydalanılmasını engelleyen kurallar da mevcut değildir. Dolayısıyla bu araçlar kullanılarak elde edilen bilgi ve verilerin kullanımı ile bu araçlar ile paylaşılan verilerin işlenmesinden yalnızca avukat sorumlu olacaktır. Burada yalnızca ortaya bir zarar çıkması değil, mesleki sorumluluklar da devreye girecektir. Avukatların her ne kadar tevkil verme gibi yetkileri bulunsa da esas olan şahsen ifa sorumluluğudur. Bu sorumluluk, işi tevkil yoluyla bir başka meslektaş yapmış olsa da vekil olan avukatın sorumluluğunu çoğu zaman ortadan kaldırmamaktadır. Bu sebeple, yapay zekâ araçlarının kullanılması ve bu yolla maddi veya manevi bir zarar doğması durumunda, şahsen ifa sorumluluğunun da ihlali doğabilir.

Avukat ve müvekkili arasındaki vekalet ilişkisinin doğal yapısından kaynaklanan müvekkil lehine davranma yükümlülüğü söz konusudur. Buraya kadar anlatılan yapay zekâ araçlarının kullanılması ile karşılaşılabilecek tüm sorunlar, avukatın, müvekkili lehine davranma zorunluluğunun da ihlali sonucunu doğurabilmektedir. Örneğin, yapay zekâ araçlarından alınacak gerçeğe

aykırı veya yanlış bilgilerin, denetlenmeden kullanılması, avukatın özen yükümlülüğünün ihlali olabileceği gibi; aynı durum, müvekkil lehine davranma yönündeki sorumlulukların da ihlalini doğurabilir. Bu yükümlülüğün ihlali, yalnızca yanlış bilgi veya gerçeğe aykırı verilerle elde edilen sonuçlarla gerçekleşmez. Kişisel verilerin öneminin anlatıldığı ve bu verilerin değerinin herkese tam olarak kavratılmaya çalışılan bir dönemde, bu verilerin bilinçsiz ve dikkatsiz şekilde yapay zekâ araçlarıyla paylaşılması da doğrudan müvekkil lehine davranma yükümlülüğünün ihlali sonucuyla karşılaşılmasına neden olacaktır. Zira kişisel verilerle ilgili kural, bu verilerin işlenmemesi yönündedir. Getirilen tüm yaptırım ve yükümlülükler, kişisel verilerin hangi durumlarda hangi şartlarda işlenebileceği şeklinde, esas kuralın istisnaları olarak yorumlanabilir. Yapay zekâ araçlarının avukatlar tarafından genel kullanım şekilleri değerlendirildiğinde; kişisel verilerin işlenmemesi yönündeki esas kuralın herhangi bir istisnası kapsamında olmadığı görülmektedir. Dolayısıyla hiçbir özen ve dikkat gösterilmeksizin herhangi bir kişisel verinin, yapay zekâ araçlarıyla doğrudan paylaşılması, avukatın müvekkili lehine davranma yükümlülüğünün de ihlali anlamına gelecektir.

Tüm bu anlatılanlar ışığında, yapay zekâ araçlarının dikkatsiz şekilde kullanılmasının gerek hukukun çeşitli alanlarını alakadar edecek biçimde uyuşmazlıklara neden olabilme potansiyeli gerek hukuki bir uyuşmazlık çıkarmadan da sosyal hayatın farklı konularında oluşturabileceği güvenlik açığı gibi çok fazla riskin aynı anda gerçekleşebileceği ifade edilmiştir. Yapay zekâ kullanan avukatlar özelinde ise tüm bu risklerin doğrudan bir uyuşmazlık konusu olması halinde ve/veya bir uyuşmazlığın çözümü sürecinde rol oynayan avukatın kullandığı yapay zekâ araçları nedeniyle mesleğe özgü doğabilecek riskler de bulunduğu özetlenmiştir.

Özellikle bireylerin kişisel verilerine hâkim olunan bir meslek olması sebebiyle yapay zekâ araçlarının barındırdığı riskler meslek faaliyetleri ve yükümlülükleri değerlendirildiğinde avukatlar özelinde çok daha büyük tehlikeleri beraberinde getirmektedir.

GÜVENLİK ÖNLEMLERİ

Avukatların yapay zekâ araçlarını kullanmasının pek çok riski beraberinde getirdiğini kabul etmekle beraber, günün şartlarının yalnızca riskler açısından değerlendirilmesi, avukatları teknolojik gelişmelerin getirdiği imkânlardan mahrum bırakmak anlamına gelecektir. Ayrıca mesleki faaliyetlerimiz çerçevesinde bu imkânlardan yararlanmamak, avukatları çağın gerisinde de bırakacaktır. Bu sebeple doğrudan yapay zekâ araçlarının kullanılmasının yasaklanması veya bu kullanımın bir şekilde kişi veya kurumlarca engellenmeye çalışılması, doğru bir yaklaşım değildir. Hatta böyle bir engelleme, büyük çerçevede insan haklarına da aykırılık teşkil edecektir.

Avukatların, bu riskler nedeniyle yapay zekâ araçlarından tamamen uzaklaşması yerine, özellikle mesleki açıdan alınabilecek tedbirleri benimseyerek kullanmaları gerekmektedir. Böylece hem avukatlar çağın imkânlarından faydalanacak hem de bu imkânların genel ve mesleğe özgü risklerinden kendilerini korumuş olacaktır.

Kişisel verilerin, yapay zekâ araçlarının en önemli besleyicisi olduğu hakkındaki anlatımlarımız nedeniyle, avukatların mesleki faaliyetlerinde yapay zekâ araçlarını kullanırken alabilecekleri güvenlik önlemlerine de kişisel veriler

hakkında yoğunlaşarak başlamak doğru olacaktır.

KVKK'nın 7.maddesi; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini düzenlemektedir. Fakat bu madde, doğrudan avukatların yapay zekâ kullanımlarına entegre edilemez. Zira maddede, hukuka uygun olarak işlenen bir kişisel verinin, işlenmesini gerektirecek sebebin ortadan kalkması halinde silinmesi, yok edilmesi veya anonim hale getirilmesinden söz edilmektedir. Oysa yapay zekâ kullanımında, işlenmesini gerektiren bir kişisel verinin varlığından söz edilemeyeceği gibi, bu işlenme şeklinin tümüyle hukuka uygun olduğundan da söz edilemez. Yine de maddenin 3.fıkrasında sözü edilen yönetmelik (Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik), bu kavramları açıklamaktadır. Bu kavramların açıklamaları avukatların yapay zekâ kullanımı sırasında kişisel verileri nasıl koruyabileceğine ışık tutmaktadır. Yönetmelik kişisel verilerin silinmesini 8.maddede *"Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.";* kişisel verilerin yok edilmesini 9.maddede *"Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir."* Ve kişisel verilerin anonim hale getirilmesini 10.maddede *"Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir."* şeklinde tanımlamaktadır. Bu tanımlar ışığında kişisel verilerin silinmesi ve yok edilmesi işlemlerinin, yapay zekâ kullanan avukatlar açısından uygun bir tedbir olmadığı açıktır. Zira bu silinme ve yok edilme işlemleri; işlenen bir kişisel verinin, işlenmesini gerektiren sebeplerin ortadan kalkması halinde bu verilere erişimin mümkün kılınmayacak hale getirilmesini ifade etmektedir. Oysa yapay zekâ araçlarının veri havuzlarında biriken bu verilerin, verileri paylaşan kişi tarafından bu havuzdan silinemeyeceği veya yok edilemeyeceği aşikardır. Zira bu yapay zekâ araçlarının doğası gereği sürekli yeni bilgi ve verilerle beslenmesinin gerekmesi, bu araçlara aktarılan verilerin de ulaşılamayacak bir hale getirilmesini mümkün kılmayacak şekilde bir yazılıma sahip olma zorunluluğunu beraberinde getirmektedir. Dolayısıyla yapay zekâ araçlarını kullanacak bir avukatın da, yalnızca prompları ile veri girişini sağlayan taraf olduğu düşünüldüğünde; kişisel verilerin silinmesi ve yok edilmesi önlemlerinin bu kullanım şeklinde, mesleki sorumluluğu ortadan kaldıracak tedbirler olmadığı açıktır.

Bununla beraber, kişisel verilerin anonim hale getirilmesi önlemi ise bu verilerin herhangi bir kimliği belirlenemeyecek hale getirilmesini ifade etmektedir. Tabii bu önlemler, kanun kapsamında veri sorumlusu olarak tanımlanan gerçek veya tüzel kişiler tarafından hukuka uygun olarak işlenmiş kişisel verilerin, işlenmesini gerektiren nedenlerin ortadan kalkması halinde, işlenmiş verilerin anonimleştirilmesini ifade etmekteyse de yapay zekâ kullanan avukatlar tarafından da uygun bir güvenlik önlemi olarak kullanılabilir bir yöntemdir. Şöyle ki; yapay zekâ araçlarına yazılan promptları, henüz bu araçlara girildiği sırada anonimleştirerek talimat girişi yapılması basit ve önemli bir güvenlik önlemi olarak değerlendirilebilir. Örneğin, bir belgenin özeti istendiğinde; bu belge içerisindeki kişisel veri sayılabilecek

mahkeme isim ve dosya numarası, kişilerin kimlik bilgileri, vekil, bilirkişi, hakim, katip gibi belgede isim veya sicil numarası bulunabilecek kişilerin bilgilerinin, belge içerisindeki anlatımlarda kişiye özgü olan ve herhangi bir kişinin belirlenebilir şekilde belgede yer alan tüm kısımların önceden kapatılarak veya silinerek yapay zeka aracına yüklenmesi gibi bir anonimleştirme işlemi yapılması, riskleri minimize ederek birtakım mesleki tehlikeleri de önlemekte faydalı olabilecektir.

Bununla beraber, genel yapay zekâ kullanımı ile avukatlara özel öneriler yapmak amacıyla yayımlanan pek çok yapay zekâ rehberi bulunmaktadır. Ülkemizde Kişisel Verileri Koruma Kurumu ve barolar tarafından düzenlenen rehberler bulunmakla beraber, uluslararası belgelerde de pek çok öneri, bu rehberlerde yer almaktadır. Bu belgelerin ortak noktası; en temel öneri olarak özellikle kişisel verilerin anonimleştirilmesi ve genelleştirilmesi gerektiği üzerinde durulmuştur. Yine bu rehberlerde ortak olarak üzerinde durulan bir diğer husus da yapay zekâ araçlarının kullanılmasında bir sakınca olmamakla beraber, avukatların bu araçları mesleki faaliyetleri çerçevesinde kullanırken mesleğin getirdiği yükümlülüklere özen göstermesi gerektiği yönündedir.

Avukatların yapay zekâ araçlarını kullanırken alabileceği bir diğer önlem de sözleşme incelemelerini detaylı olarak yapmaktır. Burada hem iş sahibi ile vekil arasında yapılan sözleşmeler hem de yapay zekâ araçlarının tedarikçi sözleşmelerinin incelenmesi önem taşımaktadır. Yukarıda belirtildiği gibi; mesleki yükümlülüklere uygun şekilde bu araçları kullanırken önemli olan hususlardan biri, gerekli anonimleştirme ve genelleştirme işlemleri yapılıyor olsa dahi müvekkili bu hususta bilgilendirmektir. Bu durum, iş sahibi ile yapılan sözleşmelerin güncellenmesi gerektiği sonucunu doğurabilmektedir. Bununla beraber, incelenmesi gereken diğer bir sözleşme de yapay zekâ araçlarının, ülkemizde sağladığı hizmet açısından sunduğu sözleşme ve benzeri belgelerdir. Bu belgelerin de ilgili aracın kullanmaya başlanmadan önce incelenmesi, büyük veri açıklarının ve yükümlülük doğuran zararların önüne geçilmesine yardımcı olacaktır.

Özellikle yalnızca avukatların kullanımına özel tasarlanmış ve çoğunlukla abonelik usulüyle hizmet veren yapay zekâ sistemlerinin, kullanıcı avukat ile yaptığı sözleşmelerin de mutlaka incelenmesi, bu sözleşmeler nezdinde veri tutulması ve paylaşılması, tedarikçinin KVKK uyumluluğu ve gerekliyse VERBİS sorgusu yapılarak gerekli önlemler alınarak bu araçların kullanılması yoluna gidilmesi gerekmektedir.

Avukatların yapay zekâ araçlarını kullanırken alabileceği önlemler özetlenmiş olup; yapılan iş ve kullanım şeklinde göre ilgili avukatın kendisine ve işin kapsamına özel olan tedbirleri alması gerektiği de önemle belirtilmelidir. Bu tedbirler genel veri güvenliğinin sağlanması, bireysel mesleki yükümlülüklerin sağlanması ve meslek kuralları çerçevesinde meslek itibarının korunması açısından önem taşımaktadır.

HUKUKİ VE ETİK SORUMLULUK

Yapay zekâ araçlarının kullanımının avukatlar açısından risk ve tehditleri özellikle kişisel veriler açısından incelenmiş olup bu riskleri yalnızca veri hukukuna indirgemek, esasen en büyük risktir. Avukatlar özelinde ortaya çıkabilecek mesleki sorumluluklar, avukatlık etiği kapsamında bireysel ve mesleki anlamda pek çok farklı yükümlülüğü de beraberinde getirmektedir.

Bu sorumluluklar kapsamında, yapay zekâ araçları nedeniyle ortaya çıkabilecek herhangi bir uyuşmazlığın ortasında kalan avukatın, yapay zekâ araçlarını kullanma yönünde yapacağı savunma, Avukatlık Kanunu ve meslek etiği gözetildiğinde yeterli değildir. Zira bu araçların pek çok açığı olduğu gibi, mevzuatımızda doğrudan bir yapay zekâ mevzuatı olmamakla beraber, pek çok düzenleme içerisinde yer alan denetim ve tedbirlerin öncelikle avukatlar tarafından alınması beklenir. Bu beklenti hem müvekkil işleri nezdinde hem de avukatlık faaliyetleri kapsamındadır.

Hukuki ve etik sorumluluk nezdinde risk analizlerinin yaptırılması, sözleşme inceleme yöntemlerinin çağın gerektirdiği yapay zekâ kullanımının risklerini minimize ederek mesleki yükümlülüklere karşı savunma mekanizması geliştirmek ve mevzuat taramalarının düzenli ve titizlikle yapılarak sürecin tümüne entegre edilmesi gerekmektedir.

Günümüzde devlet kurumlarında dahi yapay zekânın sıklıkla ilk başvurulan araç olarak kullanılmaya başlanması, hukuki ve etik sorumluluğu ortadan kaldırmamaktadır. Böyle bir düşünceyle hiçbir güvenlik tedbiri alınmadan yapay zekâ kullanımına özellikle avukatlar tarafından devam edilmesi, başta yukarıda bahsedilen riskler olmak üzere pek çok farklı tehditle de karşı karşıya kalınmasına neden olacaktır.

Yapay zekânın sorumluluğu, bu araçlar hayatımıza girdiği günden itibaren pek çok kesin tarafından ayrı ayrı ve farklı açılardan değerlendirilmiştir. Sorumlunun geliştirici, kullanıcı veya yapay zekânın bizzat kendisi olması gerektiğine ilişkin çeşitli görüş ve öneriler sunulmuştur. Henüz yerel mevzuatımızda mevcut bir yapay zekâ düzenlemesi olmadığından böyle bir sorumluluk isnadı yapmak mümkün değildir. Bununla beraber, yapay zekânın etik ilkeleri temelde bu sistemlerinin geliştiricilerine dayanmaktadır. Her ne kadar yapay zekânın doğası gereği, geliştiriciler tarafından sunulan yazılım bilgileri içerisinde edindiği bilgileri değerlendirerek kimi zaman geliştiricilerden de bağımsız bir çıktı oluşturma beklentisi bulunsa da bu etik kavramı çerçevesinde yapay zekâ nezdinde öncelikle geliştiricilere yükümlülük düşmektedir. Fakat, etik ve hukuk beraber değerlendirildiğinde; bu iki kavramın her zaman aynı sonuca varmadığı anlaşılmaktadır. Örneğin, kasten geliştiricileri tarafından genel ahlaka uygun olmayan bir etik anlayışıyla geliştirilen yapay zekâyı dahi kullanıp kullanmama iradesi veya bu kullanımda veri paylaşma iradesi tamamen kullanıcıya ait olduğundan hukuken sorumluluk farklı kişilere ait olabilecektir. Bu noktada mevcut uyuşmazlığın temelinde yatan neden oldukça önem taşımaktadır.

Yapay zekânın çıktılarının etik anlayış seyrinin, ilk olarak geliştiricinin iradesi

veya yazılım içeriği ile değerlendirilebilecek olsa da avukatlık mesleği nezdinde de etik sorumluluk tamamen avukatlık meslek etiği çerçevesinde değerlendirilecektir. Bu nedenle yapay zekânın yazılım dili, kodları veya herhangi bir teknik detayında ya da geliştiricisinin hiçbir etik aykırılığı bulunmasa da kullanım şekli ve girilen promptlar nedeniyle kullanan avukat açısından etik değerlerin ihlali gündeme gelecektir. Dolayısıyla yapay zekâ araçlarının kullanımındaki etik problemler tamamen kullanım şekline bağlı olarak ortaya çıkmaktadır.

Bununla beraber, avukatların etik sorumluluğu yanında, kullanım şekilleri hukuki sorumluluğu da doğmaktadır. Avukatlar tarafından bilinçsiz, dikkatsiz ve meslek kurallarına aykırı bir yapay zekâ kullanımı nedeniyle gelişebilecek uyuşmazlıklar maddi ve manevi zararların tazmini, cezai ve idari sorumluluklar, tüketici mahkemelerinde görülecek vekil-müvekkil ilişkilerinin uyuşmazlığı gibi sonuçlar doğurabilmektedir.

Avukatlar açısından yapay zekâ kullanımının hukuki ve etik sorumluluğunun kesiştiği noktalar da bulunmaktadır. Bu kesişim özellikle avukatların müvekkillerine karşı şeffaflık yükümlülüğünden kaynaklanmaktadır. Avukatlar, müvekkillerine karşı bu yükümlülüklerini yerine getirmediği taktirde meslek kurallarına aykırılık nedeniyle etik sorumluluk; bu aykırılıktan doğan müvekkil zararı olduğu taktirde de hukuki sorumlulukla karşı karşıya kalabilecektir.

SONUÇ

Günümüz koşullarında yapay zekânın kullanılmadığı bir meslek grubunun varlığının düşünülmesi neredeyse mümkün değildir. Tüm meslek grupları, bir şekilde mutlaka yapay zekâya başvurarak işlerini yürütmektedir. Pek çok alanda yapay zekâ ilk başvurulan ve ne yazık ki en çok güvenilen araç haline gelmiştir.

Özellikle avukatlık mesleğinin icrasında yapay zekâ araçlarının kullanımının yaygınlaşması, teknoloji şirketleri ve yazılım geliştiriciler tarafından yalnızca avukatların kullanımına özel araçların geliştirilmesine neden olmuştur. Bu yapay zekâ araçlarının özellikle avukatlara yönelik özel olarak geliştirilmesi de avukatlar tarafından yapay zekâ araçlarının kullanımını yaygınlaştırmıştır.

Bu kullanımların bilinçlendirilme eğitimlerinin yetişemeyeceği bir hızda hayatımıza girmesi nedeniyle kullanımı sırasında hukuki açıklara neden olmaktadır.

Yapay zekânın kullanım şekli konusunda, en çok karşılaşılan hukuki problem, kişisel verilerin hukuka aykırı olarak işlenmesidir. KVKK uyarınca kişisel verilerin işlenmesi, belirli kurallar çerçevesinde ele alınmış ve esas olarak işlenmesini gerektirecek geçerli bir sebebin olması, bu sebebin ortadan kalkması halinde ise işlenmiş olan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yolları hükme bağlanmıştır. Fakat yapay zekânın kullanımı sırasında paylaşılan tüm kişisel veriler, sonrasında silme, yok etme veya anonimleştirme imkânı olmaksızın işlenmektedir. Bu sebeple yapay zekâ kullanımında en çok özen gösterilmesi gereken husus, kişisel verilerin yapay zekâ ile paylaşılmamasıdır.

Yapay zekânın kullanımı sırasında işlenen verilerin yalnızca kişisel veriler olmadığı, tüzel kişilerin de verilerinin yapay zekâ araçlarıyla paylaşılması nedeniyle çeşitli hukuki uyumsuzluklar ortaya çıkabileceği ve farklı hukuk dallarında da uyuşmazlıklar doğabileceği özetlenmiştir.

Bununla beraber, bu çalışma kapsamındaki en önemli problem, avukatların yapay zekâ kullanmaları sırasında mesleki faaliyetleri sebebiyle karşılaşabilecekleri dikkat edilmesi gereken çok daha fazla husus bulunduğuna dikkat çekilmiştir.

Avukatların yapay zekâ kullanımları sırasında karşılaşabilecekleri hukuki ve etik problemlerin her zaman aynı sonucu doğurmayacağı, yapay zekâ etiğinin doğrudan bu kapsamda değerlendirilemez olduğu vurgulanmıştır. Yapay zekâ etiği ile avukatların yapay zekâ kullanımları sırasında karşılaşabilecekleri etik değerleri doğrusal olmayabilir.

Özellikle avukatların, çağın bir gereği olarak kullanacakları her türlü yapay zekâ aracın kullanmalarının hiçbir şekilde engellenemeyeceği; fakat bu araçların kullanımı sırasında gerek sosyal gerekse mesleki açıdan karşılaşılabilecek hukuki ve etik sorunların öngörülerek bunlara önlem alınması ve bu önlemler doğrultusunda dikkatle çalışmaları gerekmektedir. Bu gereklilik aynı zamanda meslek etiğinin de bir gereğidir.

KAYNAKÇA:

1. https://www.bicakhukuk.com/hukuk-hizmetlerine-yapay-zekanin-entegrasyonu/
2. https://www.genesishukuk.com/tr/yayinlar/yapay-zeka-hukuku-zkp-kvkk-veri-gizliligi
3. https://www.tnchukuk.com.tr/post/yapay-zeka-%C3%A7a%C4%9F%C4%B1nda-ki%C5%9Fisel-verileri-koruma-kvkk-hukuku
4. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/MTY5MjNmNmIwZWY3YTE.pdf
5. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ankarabarosu.org.tr/serve/file/bc4de0be-b5fa-11ef-8f94-000c29c9dfce/yapay_zeka_araclarnn_kullanm_rehberi_X1.pdf
6. https://istanbullawyerfirm.com/blog/ai-compliance-turkey
7. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.bilkent.edu.tr/server/api/core/bitstreams/3d7dc3f7-79f3-41b1-96b5-bff8fa8aa902/content

TÜRKİYE KRİPTO VARLIK PAZARI 2026: REGÜLASYONEL KONSOLİDASYON VE KURUMSAL DÖNÜŞÜM

AV. HİLAL KARAKAŞ EKER

Bu yazı, 2026 yılı eşiğinde Türkiye kripto varlık ekosistemini; sermaye yeterliliği yükümlülükleri, yargı içtihatları, kurumsal saklama disiplini ve küresel rekabet endeksleri çerçevesinde incelemektedir.

Finansal İnovasyonun Regülasyonel Evrimi

Satoshi Nakamoto'nun 2010 yılındaki vedasının üzerinden geçen 15 yılın ardından kripto varlıklar, "merkeziyetsiz finans" (DeFi) idealinden çıkarak "düzenlenmiş finansal araçlar" kategorisine dahil olmuştur. Türkiye özelinde 2026 yılı, serbest piyasa dinamiklerinin "yasa odaklı denetim" (Regulatory Compliance) ile yer değiştirdiği, sektörün "kurumsal olgunluk" sınavına tabi tutulduğu bir dönemdir.

Pazar Anatomisi: Kullanıcı ve Altyapı

Türkiye, küresel kripto adaptasyonunda öncü bir konuma sahip olsa da, bireysel ilginin hızı kurumsal ve hukuki altyapı endekslerine aynı oranda yansımamaktadır. Bybit 2025-26 verileri[1], bu yapısal tezatlığı somut rakamlarla ortaya koymaktadır: Ülkemiz, kullanıcı penetrasyonunda dünyada 15., kripto sahipliğinde ise 23. sırada yer alarak yaygın bir adaptasyon sergilemektedir. Buna karşın, kurumsal hazırlıkta 54., genel altyapı ve mevzuat uyumunda ise 64. sıraya gerilemesi, pazarın "bireysel ve kayıt dışı" karakterini koruduğuna işaret etmektedir. Mevcut tablo; yüksek bireysel talebin, regülasyonel darboğazlar ve yetersiz kurumsallaşma nedeniyle ekonomik bir kaldıraça dönüşemediğini, aksine yerli oyuncuların gelişim potansiyelini sınırlayan bir yapısal uçurum yarattığını kanıtlamaktadır.

Finansal Bariyerler

Sermaye Piyasası Kurulu (SPK) tarafından 2026 yılı için belirlenen asgari sermaye şartları, Türkiye'yi maliyet açısından en yüksek giriş bariyerine sahip pazarlar arasına taşımıştır.

Asgari Sermaye Karşılaştırması (30 Haziran 2026 Projeksiyonu)

SPK'nın takdir yetkisini kullanarak %25 ile %100 arasında artırdığı limitler, küçük ve orta ölçekli yerel oyuncular için "Regulated Extinction" (Düzenlenmiş Yok Oluş) sürecini tetiklemiştir.

Türkiye (Platform): ~7.0 Milyon USD (250 Milyon TL)

Türkiye (Saklama): ~17.5 Milyon USD (630 Milyon TL)

Dubai (VARA): 1.3 - 2.7 Milyon USD

AB (MiCA): 55.000 - 165.000 USD

Bu sermaye yoğunluğu, pazarın 2026 sonrasında banka iştirakleri ve küresel sermaye grupları arasında konsolide olacağına işaret etmektedir.

Hukuki Perspektif ve Yargı Denetimi

[1] https://assets.dlnews.com/dlresearch/Bybit-Report_The-World-Crypto-Rankings.pdf

Regülasyonun sert uygulama biçimlerine karşı yargı, "dengeleyici" bir unsur olarak öne çıkmaktadır. Özellikle Papara'nın TCMB kararına karşı[2] Ankara 25. İdare Mahkemesi'nden aldığı (9 Aralık 2025) yürütmeyi durdurma kararı, idari işlemlerin hukuki denetimi açısından emsal niteliğindedir. Bu süreç, "hukuk devleti" prensibinin teknolojik dönüşüm süreçlerinde dahi vazgeçilmez bir güvence olduğunu kanıtlamıştır.

Operasyonel Riskler ve Suçun Sosyolojik Dönüşümü

Kripto varlıkların suç gelirlerinin aklanması (AML) ve zimmet suçlarına konu olması, siber güvenlikten ziyade "etik ve sistemsel boşluklar" odağında tartışılmaktadır. Konya Kulu[3] örneğinde olduğu gibi, yerel ve bireysel düzeyde kripto varlıkların suistimal edilmesi, sistemin toplum genelinde "kontrolsüz bir finansal araç" olarak algılanmasından kaynaklanmaktadır. Bu durum, KVHS'lerin sadece teknik değil, personel güvenlik taraması ve etik denetim süreçlerini de en üst düzeye çıkarmasını zorunlu kılmaktadır.

Sonuç: 30 Haziran eşiği

2026 yılı, Türkiye kripto varlık piyasası için bir "Son Eleme" (Final Cull) niteliğindedir. 30 Haziran 2026 itibarıyla sermaye yeterliliğini kanıtlayamayan ve uyum süreçlerini tamamlamayan kuruluşların tasfiyesiyle birlikte pazar, kurumsal ve bankacılık odaklı yeni bir yapıya bürünecektir.

KAYNAKÇA:

https://assets.dlnews.com/dlresearch/Bybit-Report_The-World-Crypto-Rankings.pdf

TCMB'nin 30.10.2025 tarihli ve 11929/21528 sayılı kararı

https://spk.gov.tr/data/695546ca8f95db281807a9c3/2025-68.pdf

https://www.uaefiu.gov.ae/media/sjsfchg1/uaefiu-report-on-vas-public-version-dec-2025.pdf

https://masak.hmb.gov.tr/yaptirimlar

[2] İstanbul Cumhuriyet Başsavcılığı tarafından yürütülen bir soruşturma kapsamında Papara'ya 27.05.2025 tarihinde kayyım atanmıştır.Bu sürecin devamında TCMB'nin 30.10.2025 tarihli ve 11929/21528 sayılı kararı ile Papara'nın faaliyet izni iptal edilmiş ve bu karar 31.10.2025 tarihli Resmî Gazete'de yayımlanmıştır

[3] https://www.yenisafak.com/amphtml/gundem/adliyede-milyonlarca-liralik-zimmet-skandali-katip-tutuklandi-4776467

YASADIŞI BAHİS SUÇU KAPSAMINDA SUÇ GELİRLERİNİN AKLANMASI

AV. ELİF ŞUARA GÜNGÖR

Günümüz teknoloji ve internet çağı, Türk hukuk sisteminde ekonomik suçların boyutunu değiştirerek yasadışı bahis ve şans oyunlarını ciddi bir toplumsal ve ekonomik sorun haline getirmiştir . 7258 Sayılı Kanun ve MASAK Perspektifinde;yasadışı bahis sektörü, yasal bahis hacmini katlayacak seviyelere ulaşmış; kara para aklama, vergi kaçırma ve terörizmin finansmanı gibi ağır suçlarla doğrudan ilişkilendirilmeye başlanmıştır.

Bu kapsamda, ünlü sanatçı Serdar Ortaç örneğinde olduğu gibi, kişileri yasadışı bahse teşvik etme suçundan yargılamalar yapılmakta ve 2025 yılındaki kararlarda görüldüğü üzere hapis cezaları geri bırakılsa dahi sicile işlenebilmektedir. Kanun koyucu, bu tehlikelerle mücadele etmek amacıyla 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun ile kapsamlı yaptırımlar öngörmüştür.

1. Yasadışı Bahis Suçunun Kapsamı ve Cezai Müeyyideler 7258 sayılı Kanun'un 5. maddesi, yasadışı bahis ile ilgili fiilleri dört ana suç tipi ve bir kabahat olarak düzenlemiştir : Oynatma ve Yer Sağlama (m.5/1-a): Ruhsatsız olarak bahis oynatanlar veya buna yer ve imkân sağlayanlar 3 yıldan 5 yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılır . Yurtdışı Bağlantılı Bahse İmkân Sağlama (m.5/1-b): Yurtdışında oynatılan bahislere Türkiye'den erişim imkânı sağlayanlara 4 yıldan 6 yıla kadar hapis cezası verilir . Para Nakline Aracılık Etme (m.5/1-c): Bahis paralarının nakline bankalar, elektronik cüzdanlar veya "matikçilik" (hesap kiralama) yoluyla aracılık edenler 3 yıldan 5 yıla kadar hapis cezası alır . Reklam ve Teşvik (m.5/1-ç): Kişileri yasadışı bahse reklam yoluyla teşvik edenler 1 yıldan 3 yıla kadar hapis cezası ile karşılaşır . Ünlü sanatçı Serdar Ortaç'ın 2025 yılındaki yargılamasında bu suçtan 10 ay hapis cezası alması, konunun güncelliğini korumaktadır . Bahis Oynama (m.5/1-d): Bahis oynamak bir "suç" değil, "kabahat" kabul edilir . Ancak 2026 yılı itibarıyla öngörülen idari para cezaları 82.244 TL ile 329.106 TL gibi oldukça yüksek seviyelere ulaşmıştır .
2. İşbu suçtan elde edilen gelirin aklanması rolünde ilgili verileri açığa çıkaran MASAK, yasadışı bahis organizasyonlarını deşifre etmek için mali akışları yakından izlemektedir . 2022 verilerine göre, şüpheli işlem bildirimlerinin %37,39'u yasadışı bahis

ve kumar suçlarıyla ilgilidir . MASAK, 5549 sayılı Kanun'un 19/A maddesi uyarınca, şüpheli işlemleri analiz etmek amacıyla banka hesaplarını 7 iş günü boyunca askıya alma yetkisine sahiptir . Ancak uygulamada savcılık soruşturmalarıyla birleşen bu blokelerin kaldırılması 15 ile 60 gün arasında sürebilmektedir . Özellikle "hesap kiralama" yöntemiyle harçlığını çıkarmak isteyen öğrenciler veya düşük gelirli grupların hesapları, yüksek hacimli bahis paralarının toplanması için kullanılmakta ve bu kişiler doğrudan ağır hapis cezası tehdidi altına girmektedir .

3. Bu kapsamda şüpheli şahısların hesaplarına bloke koyulmaktadır.Blokelerin kaldırılması için,blokenin MASAK, Cumhuriyet Savcılığı veya mahkeme tarafından mı konulduğu bankadan sorgulanmalıdır.Bu sorgulama neticesinde, bloke edilen paranın yasadışı bahisle ilgisi olmadığı, yasal bir ticari işlemden veya gelirden kaynaklandığı ispat edilmelidir.Bilhassa bu hususta suçun manevi unsuru olan kasti unsur da hataya düştüğü kanıtlanırsa ki;özellikle hesabını başkasına kullandıran ancak bunun yasadışı bahis için kullanılacağını bilmeyen kişiler, TCK m.30 kapsamında "hata" hükümlerinden faydalanabilecektirler.

Yine suçtan elde edilen gelirin aklanması hususunda kripto varlıkların kullanımı yeni risk alanları oluşturmaktadır. Son yıllarda yasadışı bahis paralarının kripto varlıklara dönüştürülmesi, suçla mücadeleyi zorlaştıran yeni bir unsur olmuştur . Henüz kripto paralar Merkez Bankası tarafından resmi bir ödeme aracı olarak kabul edilmediği için, bu varlıkların nakline aracılık etmenin "yasa dışı bahiste para nakli" suçu kapsamında değerlendirilmesi tartışmalıdır; ancak bu durumun suç gelirlerinin aklanması (TCK 282) kapsamında 6-13 yıl arası hapis cezasına yol açabileceği unutulmamalıdır .

Ezcümle; Türkiye'de yasadışı bahis, sadece bireyleri mali kayba uğratmakla kalmayıp, devletin vergi gelirlerini ve kamu düzenini de tehdit etmektedir.MASAK'ın teknolojik takip kapasitesinin artması ve cezaların caydırıcı hale getirilmesi, bu suç türüyle mücadeledeki en önemli unsurlardır.