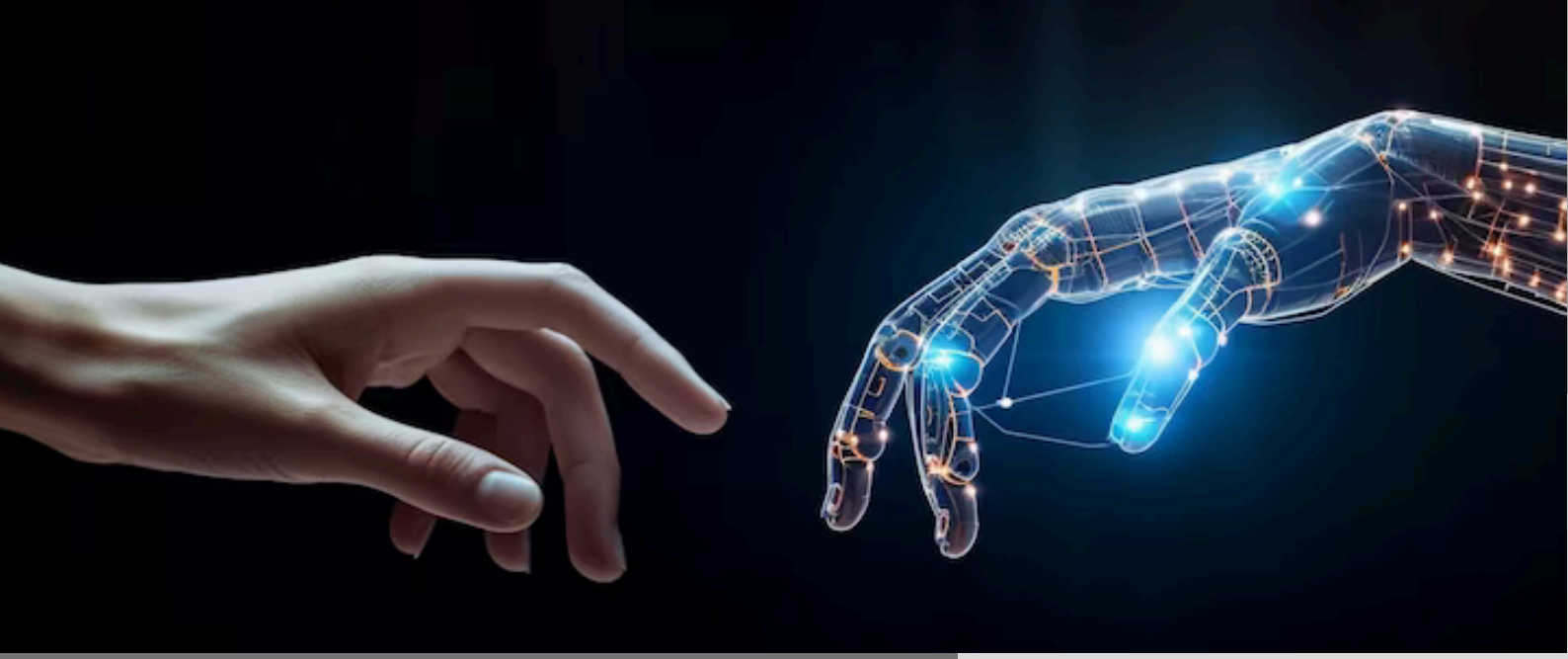




BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ



BU SAYIMIZDA

- 1 | **GÖLGE YAPAY ZEKA (SHADOW AI) VE VERİ GÜVENLİĞİ**
AV. İREM NALBANT
- 3 | **ELEKTRONİK TİCARET MEVZUATINDAKİ DEĞİŞİKLİKLER**
AV. OĞUZHAN SEYMEN
- 6 | **KRİPTO VARLIKLARDA TRAVEL RULE: DÜZENLEYİCİ ÇERÇEVE VE**
UYGULAMA SÜRECİ
AV. HİLAL KARAKAŞ EKER
- 8 | **ADLİ KOLLUK VE YAPAY ZEKA**
AV. GÖKÇEN YÜCEL

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.

GÖLGE YAPAY ZEKA (SHADOW AI) VE VERİ GÜVENLİĞİ

AV. İREM NALBANT

Bilişim teknolojileri hayatımızdaki birçok görevimizi kolaylaştırmak için bize hizmet ediyor. İş yerindeki birçok sorumluluğumuzu gerçekleştirirken arkamızda dijital izler bırakıyoruz. Genellikle tüketici tercihleri açısından ele alınan bu durum artık iş yerlerine de sıçramış durumda. Öyle ki Microsoft'un araştırmalarına göre günümüzde şirket çalışanlarının %75'i çalışırken yapay zeka araçlarını kullanıyor.¹

Bir şirket, çalışanın görevlerini yerine getirirken kullandığı bilişim elemanları sayesinde verimlilik ve yaratıcılık gibi artılar elde edebildiği gibi; bu sistemlerin güvenlik açıkları ve hukuki sınırlamalara tabi olmamasından kaynaklı veri sızıntılarına dayalı büyük risklere de maruz kalıyor. Günümüzde ciddi boyuta ulaşan bu denetimsiz bilişim sistemi kullanım durumuna "shadow IT" deniyor.

Bu yazının gündemi ise Shadow IT'nin spesifik bir dalı olan "shadow AI". Popülerleşen yapay zeka kullanımı neticesinde ticari öneme sahip birçok bilgi, çalışanlar tarafından kontrolsüz biçimde yapay zekalarla paylaşıyor. Bu yapay zekalar mevcut işin ekosistemi için tasarlanmış, güvenliği ölçülmüş ve yetkilendirilmiş sistemler olmadığından, sisteme girilen verinin akıbetini kontrol etmek mümkün olmuyor.



Şunu da belirtmek gerekir ki, çalışan bunu bilerek dahi yapmıyor olabilir. Zira artık tarayıcıda yapılan basit bir arama sonucunda dahi, "sürükle ve bırak" sistemiyle çalışan ve elde ettiği veriyi depolayan "AI tool"lar mevcut.

Yapay zekaların elde ettiği veriyi işlemesi, onunla eğitilmesi ve öğrenilmiş veriyi başka kullanıcılarla paylaşabilmesi mümkün. Bilinirliği ve kullanıcısı oldukça yüksek olan Chat GPT örneği üzerinden incelendiğinde, ChatGPT'nin arkasındaki şirket olan OpenAI, kullanıcılar aksine bir tercih yapmadığı sürece, modelin eğitimi için kullanıcının sunduğu verileri kullanıyor ve bu da özel veya hassas verilerin ifşa edilmesi potansiyeli taşıyor.

Ayrıca henüz çözülmemiş olan "AI bias" yani yapay zeka ön yargı sorunu, yazılımın hukuki regülasyonları gözetmemesi,



paylaşılan verinin ayrıca başkaca fikri mülkiyet ve sair veri haklarını ihlal edebilecek olması gibi nedenlerle, üretilen çıktının güvenilirliği de yüksek değil.²

Peki bu durumda ne yapmalı?

Bir kez güvenli ortamın dışına çıkarılıp paylaşılan verinin güvenliğinin tekrar sağlanması imkansız olduğundan, verinin en baştan bilinçli yönetilmesi gerekmektedir.

Bu açıdan, çalışanların yapay zeka yazılımları hakkında bilgilendirilmesi, şirket tarafından onaylanmamış yazılımların ne tür riskler barındırdığı, çalışanın veriyi onaylanmamış yazılımlarla paylaşması durumunda kendi sorumluluklarının ne olacağı, bu konuda bilgi alabileceği yetkililer ve sair hususlarda bilgilendirilmesi, şirketin net ve güncel bir politikası olması esastır.

Bu politika işlenebilecek veri türlerini, yasaklanmış faaliyetleri ve herkesin uyması gereken güvenlik protokollerini belirtmelidir. Çalışanları AI riskleri ve onaylanmış uygulamalar hakkında eğitmek, shadow AI risklerini azaltmanın en etkili yollarından biridir.

Çalışanlar genellikle onaylı teknolojiye boşlukları doldurmak için gölge AI araçlarına yönelirler. Anketler veya atölyeler düzenlemek, çalışanların kullandıkları onaylanmamış araçları ve çalışanı o araca yönelten nedenleri açığa çıkarır. Bu sayede, yönetim zayıflıklarını belirlemek, çalışanların onaylı çözümlerle ihtiyaçlarını giderebilmeleri için önlem almak ve ürün geliştirmek mümkün olur.³

Daha az hassas veriler için iyi bir çözüm, hem girdiler hem de çıktılar için veri gizliliği ve mahremiyet açısından garantiler sunabilen üçüncü parti yapay zeka sistemlerine erişim sağlamaktır. Daha hassas veriler için ise en güvenli yaklaşım, verilerin bulunduğu yerde AI çözümleri geliştirmektir. Bu sayede verileri harici sistemlere aktarma riski oluşmaz.

KAYNAKÇA:

1. <https://www.wiz.io/academy/shadow-ai> (1,3)
2. <https://www.linkedin.com/pulse/ai-anarchy-untold-story-shadow-data-breaches-errin-o-connor-9kpnc> (2)
3. <https://www.linkedin.com/pulse/ai-anarchy-untold-story-shadow-data-breaches-errin-o-connor-9kpnc>

ELEKTRONİK TİCARET MEVZUATINDAKİ DEĞİŞİKLİKLER

AV.OĞUZHAN SEYMEN

Elektronik ticaret(e-ticaret); gıda, kıyafet gibi fiziksel ürünlerin satıldığı perakende mağaza alışverişinden siber güvenliğe, restoran ve otel rezervasyonuna kadar internet üzerinden yapılan her türlü alışveriş demektir.

Geçtiğimiz haftalarda Türkiye Büyük Millet Meclisi Genel Kurulu hem Tüketicinin Korunması Hakkında Kanunda hem de Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun ilgili ek maddelerinde birtakım değişikliklere gitmiştir.

Bu değişikliklerden bilhassa bilişim hukukunu ilgilendiren kısmını yani e-ticarete irdelleyeceğiz:



E-ticaret mevzuatına göre;

1- Haksız ticari faaliyetlerde ne gibi yaptırımlar uygulanacaktır?

Haksız ticari uygulama; tüketicilerin karar verme süreçlerini olumsuz etkileyebilecek aldatıcı - adil olmayan iş pratikleridir.

Mesela tüketiciye yanıltıcı bilgi verilebilir, gerçek çarpıtılabilir ve tüketici Hakları ihmal edilebilir.

Sözgelimi yanıltıcı reklam, gizli ücretler, zorunlu ürün - hizmet satışı ve

koşullarının çarpıtılması, kullanıcı sözleşmelerinde gizlenen şartlar haksız ticari uygulamaya örnektir.

Yaptırım olarak e-ticaret mevzuatına aykırı haksız ticari uygulamalarda bulunulur ise 3 aya kadar tedbiren durdurma ya da 60 bin liradan 600 bin liraya kadar idari para cezasının uygulanması söz konusu olacaktır.

2- Reklam Kurulu cezalarında uzlaşma mümkün müdür?

6502 sayılı Tüketicinin Korunması Hakkında Kanunun 77/A maddesi, 2.fıkrası ile; uzlaşmanın engellenmesi iptal edildiğinden muhatapların, reklam kurulu ile uzlaşmasının önü açılmıştır.

Önemli belirtmek gerekir ki uzlaşmak, ihlali kabul anlamına gelmektedir.

İdari para cezası ödemeden uzlaşmak mümkün değildir. Çünkü indirimli de olsa mutlaka idari para cezası uygulanmaktadır ve uzlaşma metnindeki hususlar taraflarca dava konusu yapılamayacaktır.

3- Doğrudan satış hakkında nasıl bir değişiklik öngörüyorsunuz?

Doğrudan satış, tüketiciye ulaşmanın bir stratejisidir.

Arada herhangi bir perakendeci, toptancı veya distribütör olmaksızın, şirketin - satış görevlisinin, potansiyel müşterilerle doğrudan iletişime geçip ürün ve hizmet sunabilmesini sağlamaktadır.

Yine yeni Tüketici Kanunu ve E-ticaret Kanun değişikliğine göre; doğrudan satış artık kanunla düzenlenecek ve

yeni tanıma göre de tüketiciler doğrudan satıştan 30 gün içerisinde cayabileceklerdir.

4- Genel değerlendirme anlamında ilgili değişiklikler, sözleşme serbestisi ilkesine ne derece uygundur ve e-ticaret sitelerinde ne gibi genel işlem şartları olmalıdır?

Elbette Türk Ticaret Kanunu 26. Maddesi sözleşme serbestisini düzenlemiştir ve fakat aynı kanunda birtakım düzenleyici sınırlar mevcuttur.

Bu sınırlara göre de internet sitesinden alışveriş üyeliğinin - kullanımının ne şartlarda olduğuna ilişkin sözleşme yer almalıdır.

Kullanım şartlarına ilişkin bir sözleşme onaylatmamak satıcın aleyhine sonuçlar doğurabilir.



Mesafeli sözleşme yönetmeliğine göre de ön bilgilendirme yükümlülüğü olmalıdır.

Sözleşme kurulduktan sonra ve satıştan önce satıcının ve ürünün bilgileri, nitelikleri, satış bedelinin ne kadar olduğu, masrafları, ödemenin ne zaman yapılacağı ve cayma gibi klostlar yer almalıdır.

E-ticaret sitesinin kullanım koşullarının; tüketici bu koşulları onaylasın ya da onaylamasın, her kullanıcıyı bağladığına dikkat çekmek isteriz.

Nihayetinde de: iade, garanti koşulları, gizlilik ve güvenlik politikaları, verilerin

ne şekilde, ne kadar süre işlendiği ve kimlerle paylaşıldığı, E-ticaret mevzuatı ve Tüketici Kanunu kapsamında ayrıntılı olarak belirtilmelidir.

5- Genel istatistiklere göre de;

Elektronik ticaret bilgi sistemi, Ticaret Bakanlığı'nca 2017 yılından itibaren yayınlanmaya başlamış ve bu istatistikler, son 5 yılda ortalama e-ticaretin %5'inin kapıda, %35'inin havale- EFT ve %60'ının da kartlı alışveriş ile olduğu, verilere yansımıştır.

E-ticaretin en çok beyaz eşya, ev aletleri, seyahat, taşımacılık, yemek, konaklama giyim, elektronik eşya, havayolları ve gıda gibi alanlarda özellikle de beyaz eşya ve ev aletlerinde olduğu görülmüştür.

En fazla artış konaklama sektöründe, en az artış da yemek sektöründe olmuştur.

Yapılacak kanun değişikliklerinin de 24 Ekim'den itibaren 9 ay sonra yürürlüğe gireceği düşünüldüğünde, günlük hayatı kolaylaştıracağı söylenebilir.

6- E-ticaretin fırsat maliyeti ve zarar analizi nasıl yapılır?

E-ticarete genel giderler epey azaltılır, ticari gayrimenkul kiralalmaz, sadece web barındırma için uygun ücret ödenir, herhangi bir depo için kiralama ya da bir çalışan bulundurma gibi bir zorunluluk da olmaz, yalnızca alan adı ve web sitesi oluşturma gibi tipik maliyetler ortaya çıkabilir.

Alışveriş Merkezlerindeki mağazalar gibi fiziksel bir vitrin yoktur, çok fazla para harcama gibi bir endişe de yoktur, web arayüzü en etkileyici vitrindir ve çevrimiçi satın almalar başlar.

Fiziken sınırlı bir çevre sahipken e-ticaret ile çok daha geniş bir kitle ulaşır Avrupa Amerika'ya kadar müşteri portföyü oluşturulabilir.

Dezavantajlara gelirsek potansiyel güvenlik tehditleri vardır, müşterinin

kredi ve banka kartı bilgileri riske atılabilir rekabet yönünden dezavantaj ürün taklidi yapılabilmesi ve aynı sektördeki başka isimlerin sizin markanızı taklit etmesi ya da sizin alan adınızı kullanarak sizin müşterilerinizi ele geçirerek reklam yapması gibi rekabet ihlali riski olabilir.

Bilgi teknolojileri yönünden yaşanan sorunlar, daha fazla maliyet ve müşteri kaybına yol açabilir.

Nakliye lojistiği en yüksek maliyetli giderler arasındadır ve kusursuz bir nakliye çözümü kolay değildir.

E-ticaret yapılırken fiziken bir mağaza işletmek gibi müşteri ile bire bir bağlantı kurmak ve müşteriye kişisel dokunuş sunmak mümkün olmayabilir.

KAYNAKÇA:

1. * dsd.org.tr/dogrudan-satis-nedir/
2. * hukukvebilisim.org/turkiye-e-ticaret-raporu
3. * sezgenhukuk.com/e-ticarette-haksiz-ticari-uygulama
4. * eticaret.gov.tr/mevzuat,
5. * pazarlama30.com/e-ticaretin-avantajlari-ve-dezavantajlari-nelerdir/#google_vignette

KRİPTO VARLIKLARDA TRAVEL RULE: DÜZENLEYİCİ ÇERÇEVE VE UYGULAMA SÜRECİ

AV. HİLAL KARAKAŞ EKER

Giriş

Kripto varlık ekosisteminin hızla büyümesiyle birlikte, bu alandaki düzenleyici gereksinimler de giderek daha fazla önem kazanmaktadır. Özellikle suç gelirlerinin aklanması, terör finansmanının önlenmesi ve kayıt dışı ekonomiyle mücadele konularında uluslararası kuruluşlar, finansal düzenleyicilere önemli yükümlülükler getirmektedir. Bu bağlamda, Mali Eylem Görev Gücü (FATF) tarafından yayımlanan 16 numaralı tavsiye kararı doğrultusunda geliştirilen **Travel Rule (Seyahat Kuralı)**, kripto varlık transferlerinde gönderici ve alıcı bilgilerinin paylaşılmasını zorunlu kılan bir düzenleme olarak ortaya çıkmıştır. Türkiye'de de bu kurala uygun olarak 24 Aralık 2024 tarihinde, 9305 sayılı Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliği'ne Kripto Varlık Transferleri başlıklı 24/A maddesi eklenmiştir. İlgili madde 25 Şubat 2025 itibarıyla yürürlüğe girecektir.

Travel Rule'un amacı, geleneksel finans sisteminde olduğu gibi kripto varlık hizmet sağlayıcılarının (KVHS) belirli bir tutarın üzerindeki transfer işlemlerinde müşteri bilgilerini alıcı tarafa iletilmesini sağlamaktır. Türkiye'de yayımlanan yönetmeliğe göre, 15.000 TL ve üzeri kripto varlık transferlerinde şu bilgilerin paylaşılması zorunlu hale gelmiştir:

- Gönderenin kimlik bilgileri (Adı-soyadı, tüzel kişi ise unvanı, diğer teşekküller için tam adı)
- Cüzdan adresi (Yoksa işlemle ilgili referans numarası)
- Adres, doğum yeri ve tarihi, müşteri numarası veya T.C. kimlik numarası gibi tanımlayıcı bilgilerden en az biri
- Alıcı taraf için de yukarıdaki bilgilerin sağlanması

Bu düzenleme, FATF standartlarına uyum sağlamak amacıyla getirilmiş olup, bilgilerin transferle eş zamanlı ve güvenli şekilde paylaşılması gerekmektedir. Bilgilerin iletiminde dağıtık defter teknolojisi (DLT), bağımsız mesajlaşma platformları veya API tabanlı çözümler gibi teknolojik araçların kullanımı öngörülmektedir.



Türkiye'deki Mevzuat Değişiklikleri ve Travel Rule Uygulaması Türkiye'de MASAK tarafından yapılan düzenlemeler, FATF'ın belirlediği standartlara uyum sağlamak amacıyla geliştirilmiştir. Bu doğrultuda, kripto varlık hizmet sağlayıcıları finansal kuruluşlar kategorisine alınmış ve MASAK uyum programı hazırlamakla

yükümlü kılınmıştır. Özellikle müşteri tanıma (KYC) süreçleri sıkılaştırılmış, kripto varlık transferlerinde gönderici ve alıcı kimlik doğrulama zorunluluğu getirilmiştir.



Özetle, Türkiye'de yürürlüğe girecek Travel Rule düzenlemesi şu yükümlülükleri içermektedir:

*Kripto Varlık Hizmet Sağlayıcılar tarafından 15.000 TL ve üzeri transferler işlemine ilişkin mesajlarda, gönderenin ve alıcının adı soyadı/unvanı, cüzdan adresi ve adres/doğum yeri/tarihi/müşteri numarası gibi kimlik bilgilerinin doğru bir şekilde iletilmesi ve teyit edilmesi zorunludur.

*15.000 TL altı transferlerde, gönderen ve alıcının adı soyadı/unvanı ve cüzdan adresi bilgileri iletilmelidir, teyit zorunluluğu yoktur.

*Kripto varlık hizmet sağlayıcıları, eksik bilgi içeren transferleri iade etmekle yükümlüdür.

*Transfer emri veren kuruluştan nihai alıcıya kadar tüm aracılar, gönderici bilgilerini eksiksiz olarak iletmek zorundadır.

*Gönderici ve alıcı bilgileri güvenli bir şekilde ve eş zamanlı olarak iletilmelidir.

*Kripto varlık hizmet sağlayıcıları, kendi bünyelerinde kayıtlı olmayan cüzdanlara yapılan transferlerde,

müşterilerinden gönderici/alıcı bilgileri hakkında beyan almalıdır.

*Yurt dışında yerleşik ve bilgi paylaşım yükümlülüğü bulunmayan kuruluşlardan yapılan transferlerde de müşteriden beyan alınmalıdır.

*Kripto varlık hizmet sağlayıcıları, risk temelli yaklaşım çerçevesinde ek bilgi ve belge talep edebilir, şüpheli durumlarda transferi engelleyebilir veya iş ilişkisini sonlandırabilir.

Travel Rule'un uygulanması, kripto varlık piyasasında şeffaflığı ve düzenleyici uyumu artırmayı amaçlamaktadır. Türkiye'de yürürlüğe giren Tedbirler Yönetmeliği'nin 24/A maddesi, kripto transferlerinde FATF standartlarına uyumu sağlayarak suç gelirlerinin aklanması, terör finansmanı ve kayıt dışı ekonomiyle mücadelede önemli bir adım olarak değerlendirilmektedir. Bununla birlikte, düzenlemenin KVHS'ler için operasyonel yük getireceği, veri gizliliği ve teknik entegrasyon zorlukları doğurabileceği de göz önünde bulundurulmalıdır.

Kripto varlık ekosisteminin gelişimiyle birlikte, uluslararası standartlara uyum sağlamak amacıyla düzenlemelerde daha fazla güncelleme ve teknik çözüm geliştirilmesi beklenmektedir. Türkiye'deki KVHS'lerin, düzenleyici gereksinimlere uygun altyapıları oluşturması ve uyumluluk süreçlerini hızlandırması büyük önem taşımaktadır. 2025 ve sonrasında, kripto düzenlemelerinin hem ulusal hem de uluslararası düzeyde daha da sıklaştırılması beklenmektedir.

ADLİ KOLLUK VE YAPAY ZEKA

AV. GÖKÇEN YÜCEL

Özet

Bu makale, yapay zeka teknolojilerinin adli kolluk faaliyetlerinde kullanımını ve bu kullanımın insan hakları üzerindeki etkilerini incelemektedir. Yapay zeka tabanlı araçlar, adli soruşturmalarda delil toplama, şüpheli tespiti ve suç analizi gibi faaliyetlerde kullanılmaktadır. Ancak bu teknolojilerin yanlış veya yanlış şekilde kullanımı kişisel verilerin mahremiyetinin ihlali, ayrımcılık ve insan hakları ihlallerine yol açabilmektedir. Makalenin sonunda, insan hakları odaklı bir yaklaşımla yapay zeka teknolojilerinin kolluk faaliyetlerinde etik ve hukuki standartlara uygun olarak kullanılması için gerekli önlemler tartışılmaktadır.

Abstract

This article examines the use of artificial intelligence (AI) technologies in judicial law enforcement activities and their implications for human rights. AI-based tools are employed in activities such as evidence collection, suspect identification, and crime analysis. However, the misuse or biased application of these technologies may lead to violations of security of personal data, discrimination, and human rights abuses. The article concludes with recommendations for the ethical and legal use of AI technologies in law enforcement, emphasizing a human rights-centered approach.

Giriş

Yapay zeka teknolojileri, kamu sektöründe olduğu gibi kolluk faaliyetlerinde de önemli bir yer edinmiştir. Özellikle adli kolluk görevlerinde, teknolojinin sağladığı hız ve doğruluk sayesinde delil toplama, suç analizi ve şüpheli profillemeye gibi faaliyetlerde yeni yöntemler geliştirilmiştir. Bununla birlikte, bu teknolojilerin insan hakları üzerindeki etkileri, etik ve hukuki boyutlarıyla

dikkatlice ele alınmalıdır. Bu makale, yapay zeka teknolojilerinin adli kolluk faaliyetlerindeki rolünü ve karşılaşılabilecek sorunları temel bir şekilde ele almayı amaçlamaktadır.

Adli Kolluk ve Yapay Zeka

1. Bilirkişi İncelemesi ve Keşfe İlişkin Adli Kolluk Faaliyetleri

Adli kolluk faaliyetlerinde bilirkişi incelemeleri, olay yerinde toplanan delillerin detaylı analizini gerektirir. Yapay zeka teknolojileri, özellikle fiziksel delillerin dijital analizinde büyük kolaylık sağlamaktadır. DNA analizi, parmak izi tespiti ve biyometrik veri eşleştirmesi gibi işlemler, yapay zeka destekli algoritmalarla daha hızlı ve kesin bir şekilde gerçekleştirilebilmektedir. Bununla birlikte, bu sistemlerin algoritmik yanlışlık ve veri gizliliği risklerini taşımaması için dikkatli bir şekilde tasarlanması gereklidir.

2. Kişi Hürriyetini Sınırlandıran Koruma Tedbirlerine İlişkin Faaliyetler

Şüphelilerin izlenmesi ve yakalanması gibi faaliyetlerde yapay zeka, büyük veri analizi ve davranış profillemeye ile destek sağlar. Ancak, bu teknolojilerin doğru şekilde kullanımı, temel hak ve özgürlükleri korumak için etik kurallar ve yasal düzenlemelerle sınırlandırılmalıdır. Örneğin, kamusal alanlarda kullanılan yüz tanıma teknolojileri, doğru amaçlar için kullanılmadığında ciddi insan hakları ihlalleriyle sonuçlanabilir.

3. Arama ve El Koymaya İlişkin Faaliyetlerde Yapay Zeka

Adli bilişim uzmanları, yapay zeka kullanarak bilgisayarlarda, dijital cihazlarda ve veri tabanlarında arama yapabilmektedir. Yapay zeka destekli araçlar, büyük miktardaki veri arasında ilgili olanları hızlıca bulabilir ve analiz edebilir. Ancak, bu süreçlerin kişisel veri koruma kanunlarına uygun olması büyük önem taşır.

4. Modern Delil Elde Etme Yöntemleri ve Yapay Zeka

Modern delil elde etme yöntemlerinde, yapay zeka teknolojileri, iletişim tespiti, teknik araçlarla izleme ve gizli soruşturmacıların kullanımında önemli bir rol oynamaktadır. Telekomünikasyon verilerinin analizi ve kritik suç noktalarının tespiti, yapay zeka algoritmalarının etkin bir şekilde uygulandığı alanlardandır.

5. "Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law." Council of Europe. Accessed January 21, 2025. <https://rm.coe.int>.

Sonuç

Yapay zeka teknolojilerinin adli kolluk faaliyetlerinde kullanımı, önemli faydalar sağlasa da etik, hukuki ve teknik zorlukları da beraberinde getirmektedir. İnsan haklarına duyarlı bir kolluk yaklaşımı için temel olarak şu tedbirlerin alınması önerilmektedir:

1. Algoritmaların ayrımcılığı önleyecek şekilde tasarlanması ve şeffaflık ilkesiyle uygulanması.
2. Yapay zeka kullanımını düzenleyen yasal çerçevelerin geliştirilmesi.
3. Kolluk personelinin bu teknolojilere ilişkin eğitilmesi ve farkındalık düzeyinin artırılması.

Bu öneriler, yapay zeka tabanlı sistemlerin etkin ve insan haklarına uygun bir şekilde kullanılmasına yardımcı olacaktır.

KAYNAKÇA

1. Yücel, Gökçen. *Yapay Zeka Teknolojilerinin Kolluk Faaliyetlerinde Kullanımı*. Ankara: Yetkin Yayınları, 2024.
2. "EU AI Act: First Regulation on Artificial Intelligence." European Parliament. Accessed January 20, 2025. <https://www.europarl.europa.eu>.
3. Madhavan, Radhika. "Artificial Intelligence in Policing – Use-Cases, Ethical Concerns, and Trends." *Emerj Artificial Intelligence Research*. Accessed January 21, 2025. <https://emerj.com>.
4. Brynjolfsson, Erik, and McAfee, Andrew. "The Business of Artificial Intelligence." *Harvard Business Review*, 2017.