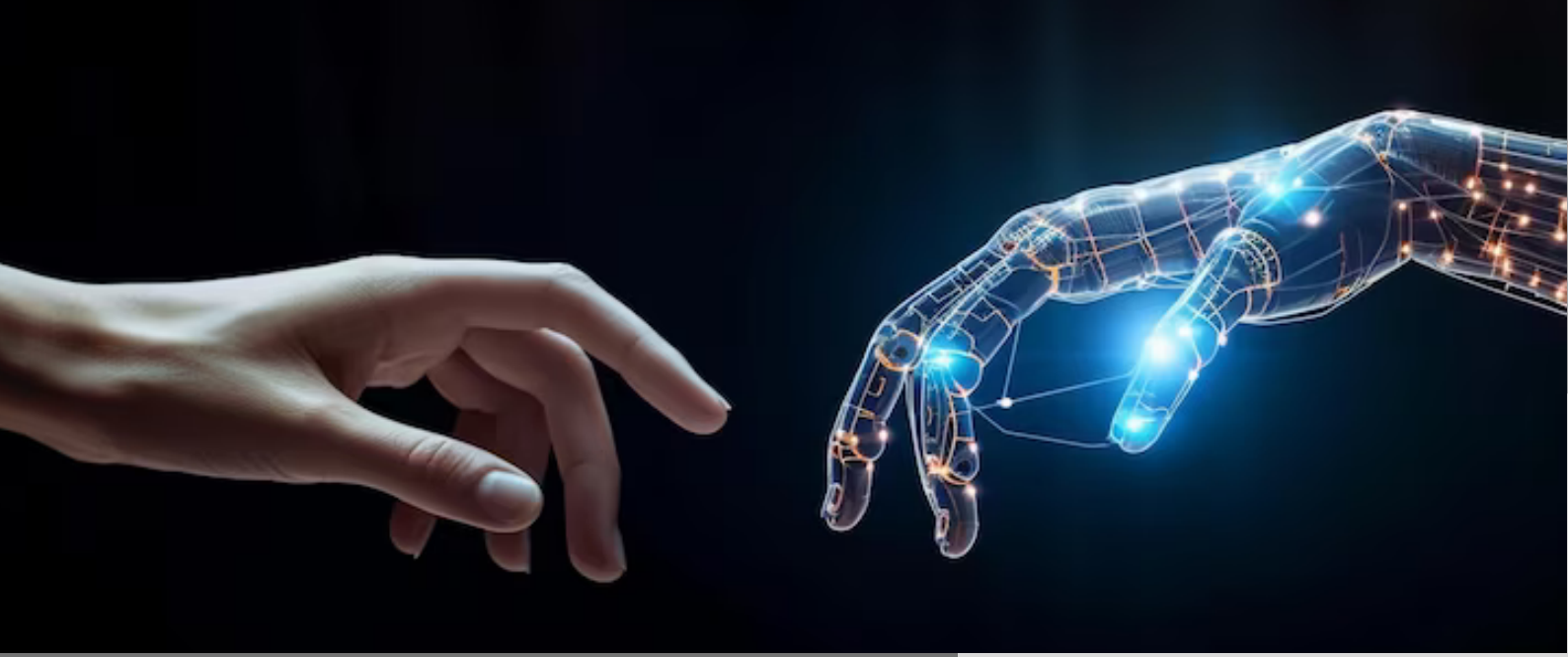




BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ



BU SAYIMIZDA

- 1 | YAPAY ZEKANIN EĞİTİM VE SAĞLIK ALANINDA ETİK VE GÜVENİLİR KULLANIMI
AV. GÖKÇEN YÜCEL
- 5 | BEYİN DALGALARINA İLİŞKİN VERİ KORUMA YASALARINDA İKİNCİ DALGA: CALIFORNIA
AV. İREM NALBANT
- 7 | POS CİHAZLARINDAKİ SATIŞ DIŞI İŞLEMLERDE VERGİSEL BOYUT
AV. OĞUZHAN SEYMEN
- 9 | TÜRKİYE'DE SİBER GÜVENLİK VE YENİ KANUN DÜZENLEMELERİ
AV. AHMET KALKAN

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.

YAPAY ZEKANIN EĞİTİM VE SAĞLIK ALANINDA ETİK VE GÜVENİLİR KULLANIMI

AV. GÖKÇEN YÜCEL

<https://www.linkedin.com/in/gokcen-yucel-99426a7b/>

Özet

Yapay zeka (YZ), son yıllarda eğitim ve sağlık alanlarında önemli bir dönüşüm aracı haline gelmiştir. Bu teknolojinin etik ve güvenilir bir şekilde kullanılması, toplumsal faydayı artırırken potansiyel riskleri minimize etmek açısından kritik öneme sahiptir. Bu makalede, yapay zekanın eğitim ve sağlık alanlarındaki uygulamaları incelenmekte, etik dışı kullanım örnekleri ele alınmakta ve bu tür kullanımlara karşı alınabilecek tedbirler ve güvenlik önlemleri tartışılmaktadır. Makale, yapay zekanın etik ve güvenilir kullanımına ilişkin uluslararası standartlar ve akademik çalışmalar ışığında bir çerçeve sunmayı amaçlamaktadır. Ayrıca, ISO'nun güvenilir yapay zeka standartlaştırma çalışmalarına da yer verilerek, bu alandaki uluslararası çabaların etik ve güvenilir yapay zeka geliştirilmesine katkıları incelenmektedir.

Giriş

Yapay zeka, insan zekasını taklit eden ve öğrenebilen sistemlerin geliştirilmesini içeren bir bilim dalıdır. Son yıllarda, yapay zeka teknolojileri eğitim ve sağlık gibi kritik alanlarda yaygın bir şekilde kullanılmaya başlanmıştır. Ancak, bu teknolojinin etik ve güvenilir bir şekilde kullanılması, toplumsal faydayı artırırken potansiyel riskleri minimize etmek açısından büyük önem taşımaktadır. Bu makale, yapay zekanın eğitim ve sağlık alanlarındaki uygulamalarını inceleyerek, etik dışı kullanım örneklerini ele alacak ve bu tür kullanımlara karşı alınabilecek tedbirler ve güvenlik önlemlerini tartışacaktır. ISO'nun güvenilir yapay zeka standartlaştırma çalışmalarına da değinilerek, bu alandaki uluslararası çabaların etik ve güvenilir yapay zeka geliştirilmesine katkıları incelenecektir.

Yapay Zeka Kavramı

Yapay zeka, insan zekasını taklit eden ve öğrenebilen sistemlerin geliştirilmesini içeren bir bilim dalıdır. Yapay zeka sistemleri, büyük veri setlerini analiz ederek, desenleri tanımlayabilir ve bu desenlere dayalı olarak kararlar alabilir (Russell & Norvig, 2020). Yapay zeka, makine öğrenmesi, derin öğrenme, doğal dil işleme gibi alt dallara ayrılır. Bu teknolojiler, eğitim ve sağlık gibi alanlarda önemli bir dönüşüm aracı haline gelmiştir. Yapay zeka, özellikle büyük veri analizi, otomasyon ve kişiselleştirilmiş hizmetler sunma konusunda büyük bir potansiyele sahiptir. Ancak, bu teknolojinin etik ve güvenilir bir şekilde kullanılması, toplumsal faydayı artırırken potansiyel riskleri minimize etmek açısından kritik öneme sahiptir.



Eğitim Alanında Yapay Zeka Uygulamaları

Yapay zeka, eğitim alanında öğrenme süreçlerini kişiselleştirme, öğrenci performansını değerlendirme ve eğitim içeriği oluşturma gibi çeşitli uygulamalarla kullanılmaktadır. Örneğin, yapay zeka tabanlı öğrenme sistemleri, öğrencilerin öğrenme stillerine ve ihtiyaçlarına göre kişiselleştirilmiş eğitim içerikleri sunabilir (Luckin et al.,

2016). Ayrıca, yapay zeka, öğrenci performansını değerlendirmek ve öğrenme süreçlerini optimize etmek için kullanılabilir. Bu tür uygulamalar, eğitimde verimliliği artırırken, öğrencilerin bireysel ihtiyaçlarını karşılamaya yardımcı olur.

Yapay zeka, öğretmenlerin iş yükünü hafifletmek için de kullanılabilir. Örneğin, yapay zeka tabanlı otomatik sınav değerlendirme sistemleri, öğretmenlerin zamanını önemli ölçüde azaltabilir (Holmes et al., 2019). Ayrıca, yapay zeka, öğrencilerin öğrenme süreçlerini izlemek ve öğrenme güçlüklerini erken aşamada tespit etmek için kullanılabilir. Bu tür uygulamalar, öğrencilerin akademik başarısını artırmaya yardımcı olabilir.

Bununla birlikte, yapay zekanın eğitim alanında kullanımı bazı etik sorunları da beraberinde getirmektedir. Örneğin, öğrencilerin kişisel verilerinin toplanması ve kullanılması, mahremiyet ihlallerine yol açabilir (Zimmer, 2010). Ayrıca, yapay zeka tabanlı sistemlerin önyargılı kararlar vermesi, öğrenciler arasında adaletsizliklere neden olabilir. Bu nedenle, yapay zekanın eğitim alanında kullanımı sırasında etik ilkelerin göz önünde bulundurulması büyük önem taşımaktadır.

Sağlık Alanında Yapay Zeka Uygulamaları

Yapay zeka, sağlık alanında teşhis, tedavi ve hasta bakımı gibi çeşitli uygulamalarla kullanılmaktadır. Örneğin, yapay zeka tabanlı teşhis sistemleri, tıbbi görüntüleri analiz ederek hastalıkları erken evrede tespit edebilir (Topol, 2019). Ayrıca, yapay zeka, hastaların tedavi süreçlerini optimize etmek ve kişiselleştirilmiş tedavi planları oluşturmak için kullanılabilir. Bu tür uygulamalar, sağlık hizmetlerinin kalitesini artırırken, hastaların yaşam kalitesini iyileştirmeye yardımcı olur.

Yapay zeka, sağlık alanında ilaç keşfi ve geliştirilmesi süreçlerinde de kullanılmaktadır. Örneğin, yapay zeka tabanlı sistemler, potansiyel ilaç

adaylarını hızlı bir şekilde tarayarak, ilaç geliştirme süreçlerini hızlandırabilir (Jumper et al., 2021). Ayrıca, yapay zeka, hastaların sağlık verilerini analiz ederek, bireysel risk faktörlerini belirleyebilir ve önleyici tedbirler önerebilir. Bu tür uygulamalar, sağlık hizmetlerinin daha etkili ve verimli bir şekilde sunulmasını sağlayabilir.

Ancak, yapay zekanın sağlık alanında kullanımı bazı etik sorunları da beraberinde getirmektedir. Örneğin, hastaların sağlık verilerinin toplanması ve kullanılması, mahremiyet ihlallerine yol açabilir (Price & Cohen, 2019). Ayrıca, yapay zeka tabanlı sistemlerin önyargılı kararlar vermesi, hastalar arasında adaletsizliklere neden olabilir. Bu nedenle, yapay zekanın sağlık alanında kullanımı sırasında etik ilkelerin göz önünde bulundurulması büyük önem taşımaktadır.



Eğitim ve Sağlık Alanında Etik Dışı Yapay Zeka Kullanımı

Yapay zekanın eğitim ve sağlık alanlarında etik dışı kullanımı, önemli riskler taşımaktadır. Yukarıda ifade edildiği üzere, yapay zeka tabanlı öğrenme sistemleri, öğrencilerin kişisel verilerini toplayarak bu verilerin kötüye kullanılmasına sebep olabilir (Zimmer, 2010). Benzer şekilde, yapay zeka tabanlı teşhis sistemleri, hastaların tıbbi verilerini yanlış yorumlayarak yanlış teşhislere yol açabilir. Bu tür etik dışı kullanımlar, bireylerin mahremiyetini ihlal edebilir ve temel hak ve hürriyetleri zedeleyebilir.

Ayrıca, yapay zeka tabanlı sistemlerin önyargılı kararlar vermesi, eğitim ve

sağlık alanlarında adaletsizliklere neden olabilir. Örneğin, yapay zeka tabanlı öğrenci değerlendirme sistemleri, belirli öğrenci gruplarını dezavantajlı duruma düşürebilir (O'Neil, 2016). Benzer şekilde, yapay zeka tabanlı teşhis sistemleri, belirli hasta gruplarını yanlış teşhis edebilir. Bu tür etik dışı kullanımlar, toplumsal eşitsizlikleri artırabilir ve bireylerin temel haklarını ihlal edebilir.

Etik Dışı Yapay Zeka Kullanımına İlişkin Alınabilecek Tedbirler ve Güvenlik Önlemleri

Yapay zekanın etik dışı kullanımına karşı alınabilecek tedbirler ve güvenlik önlemleri, bu teknolojinin güvenilir bir şekilde kullanılmasını sağlamak açısından kritik öneme sahiptir. Öncelikle, yapay zeka sistemlerinin geliştirilmesi ve kullanımı sırasında etik ilkelerin göz önünde bulundurulması gerekmektedir. Bu ilkeler, şeffaflık, hesap verebilirlik, adalet ve mahremiyet gibi temel değerleri içermelidir (Floridi et al., 2018). Ayrıca, yapay zeka sistemlerinin denetlenmesi ve düzenlenmesi için uluslararası standartların oluşturulması önemlidir. Bu standartlar, yapay zeka sistemlerinin etik ve güvenilir bir şekilde kullanılmasını sağlamak için gerekli çerçeveyi sunabilir.

Yapay zeka sistemlerinin geliştirilmesi sırasında, veri setlerinin çeşitliliği ve temsiliyeti göz önünde bulundurulmalıdır. Bu, yapay zeka sistemlerinin önyargılı kararlar vermesini önlemek açısından kritik öneme sahiptir (Mehrabi et al., 2021). Ayrıca, yapay zeka sistemlerinin karar verme süreçlerinin şeffaf olması ve bu süreçlerin denetlenebilir olması gerekmektedir. Bu, yapay zeka sistemlerinin güvenilirliğini artırmak açısından önemlidir.

Yapay zeka sistemlerinin kullanımı sırasında, bireylerin mahremiyet haklarının korunması büyük önem taşımaktadır. Bu nedenle, yapay zeka sistemlerinin kişisel verileri toplama ve kullanma süreçlerinde, mahremiyet koruma önlemleri alınmalıdır (GDPR, 2018). Ayrıca, yapay zeka sistemlerinin

kullanımı sırasında, bireylerin bilgilendirilmiş onaylarının alınması gerekmektedir. Bu, bireylerin haklarının korunması açısından önemlidir.

ISO'nun Güvenilir Yapay Zeka Standartlaştırma Çalışmaları

Uluslararası Standartlar Örgütü (ISO), yapay zeka alanında güvenilir ve etik kullanımı desteklemek amacıyla çeşitli standartlar geliştirmektedir. ISO/IEC TR 24027:2021 standardı, yapay zeka sistemlerindeki önyargıların ölçülmesi ve yönetilmesine yönelik yöntemler içermektedir (ISO, 2021). Bu standart, yapay zeka sistemlerinin adil ve şeffaf bir şekilde çalışmasını sağlamak amacıyla veri kalitesi ve model doğruluğu gibi konularda rehberlik sunmaktadır. Ayrıca, ISO'nun yapay zeka etik ilkeleri ve gereksinimleri üzerine yaptığı çalışmalar, Avrupa Birliği'nin güvenilir yapay zeka rehberi ile uyumlu bir şekilde geliştirilmektedir (European Commission, 2019).

ISO'nun bu çalışmaları, yapay zeka sistemlerinin geliştirilmesi ve kullanımı sırasında etik ilkelerin göz önünde bulundurulmasını sağlamak amacıyla önemli bir adım olarak değerlendirilebilir. Özellikle, yapay zeka sistemlerinin önyargılarını ölçmek ve yönetmek için geliştirilen yöntemler, bu sistemlerin adil ve şeffaf bir şekilde çalışmasını sağlamak açısından kritik öneme sahiptir.

Sonuç

Yapay zeka, eğitim ve sağlık alanlarında önemli bir dönüşüm aracı haline gelmiştir. Ancak, bu teknolojinin etik ve güvenilir bir şekilde kullanılması, toplumsal faydayı artırırken potansiyel riskleri minimize etmek açısından kritik öneme sahiptir. Bu makalede, yapay zekanın eğitim ve sağlık alanlarındaki uygulamaları incelenmiş, etik dışı kullanım örnekleri ele alınmış ve bu tür kullanımlara karşı alınabilecek tedbirler ve güvenlik önlemleri tartışılmıştır. Yapay zekanın etik ve güvenilir kullanımına ilişkin uluslararası standartlar ve akademik çalışmalar ışığında bir

çerçeve sunulmuştur. Ayrıca, yapay zekanın bu alanlardaki gelecekteki potansiyeli ve karşılaşılabilecek zorluklar da detaylı bir şekilde incelenmiştir. ISO'nun güvenilir yapay zeka standartlaştırma çalışmalarına da değinilerek, bu alandaki uluslararası çabaların etik ve güvenilir yapay zeka geliştirilmesine katkıları incelenmiştir. Yapay zekanın eğitim ve sağlık alanlarında etik ve güvenilir bir şekilde kullanılması, toplumsal faydayı artırırken, bireylerin haklarını korumak açısından büyük önem taşımaktadır.

KAYNAKÇA:

1. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689-707.
2. GDPR. (2018). General Data Protection Regulation. *Official Journal of the European Union*.
3. Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Center for Curriculum Redesign.
4. ISO. (2021). ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making. *International Organization for Standardization*.
5. Jumper, J., Evans, R., Pritzel, A., Green, T., Figurnov, M., Ronneberger, O., ... & Hassabis, D. (2021). Highly accurate protein structure prediction with AlphaFold. *Nature*, 596(7873), 583-589.
6. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). *Intelligence Unleashed: An argument for AI in Education*. Pearson Education.
7. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys (CSUR)*, 54(6), 1-35.
8. O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.
9. Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25(1), 37-43.
10. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*. Pearson.
11. Topol, E. J. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books.
12. Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology*, 12(4), 313-325.

BEYİN DALGALARINA İLİŞKİN VERİ KORUMA YASALARINDA İKİNCİ DALGA: CALIFORNIA

AV. İREM NALBANT

Geçmiş bir yazımızda beyin dalgalarının kişisel veri olarak kabulüne ilişkin ilk resmi düzenlemeleri ve beyin dalgalarının veri niteliği üzerine yazmıştık. Bu yazımızda, Silikon Vadisine de ev sahipliği yapmakta olan ABD-California eyaletinin beyin dalgalarına ilişkin düzenlemesini inceleyeceğiz.

Beyin dalgalarını ölçen cihazlardan, elektriksel aktiviteyi veya kan akışını izleyenlere kadar, beyin faaliyetlerinin takip edilebildiğini artık biliyoruz. Bilim insanları, bu verileri felçli insanlara uzuvlarını hareket ettirmelerine veya sadece düşünce yoluyla iletişim kurmalarına yardımcı olacak sinyallere dönüştürmeyi başardılar.



Ancak, elbette her kişisel veri gibi bu verilerin de sağlık hizmetlerinin ötesinde de kullanımları açığa çıktı. Günümüzde, tüketiciler beyinlerinin nasıl çalıştığını öğrenmelerini ve sakin hissetmelerine yardımcı olmasını sağlayan kulaklıklar satın alabiliyorlar. İşverenler, çalışanlarının ne kadar uyanık olduklarını izlemek için cihazlar kullanıyor, okullar ise öğrencilerin dikkatlerinin yerinde olup olmadığını kontrol ediyor.

Beyin verileri diğer birçok kişisel veriye kıyasla çok daha hassas ve değerli. Beyin dalgası dendiğinde sadece teknik bir işleyişin sinyallerinin değil; nasıl düşündüğümüzü ve hissettiğimizi ve en

içsel tercih ve arzularımızı gösteren sinyallerin söz konusu olduğunu hatırlamakta fayda var. Bu nedenle, California yasasının zihinsel gizliliği nasıl koruyabileceğine ve bu konuda ne kadar yol almamız gerektiğine bir göz atalım.

Yeni yasa tasarısı, 2018 tarihli California Tüketici Gizliliği Yasası'nı değiştiriyor ve tüketicilere, işletmeler tarafından toplanan kişisel bilgiler üzerinde haklar tanıyor. "Kişisel bilgi" terimi zaten biyometrik verileri (yüzünüz, sesiniz veya parmak izleriniz gibi) içeriyordu. Şimdi ise açıkça sinirsel verileri de kapsıyor.

Yasa, sinirsel verileri "bir tüketicinin merkezi veya periferik sinir sisteminin aktivitesini ölçerek üretilen ve sinirsel olmayan bilgilerden çıkarılmayan bilgiler" olarak tanımlıyor. Başka bir deyişle, bir kişinin beyninden veya sinirlerinden toplanan veriler.

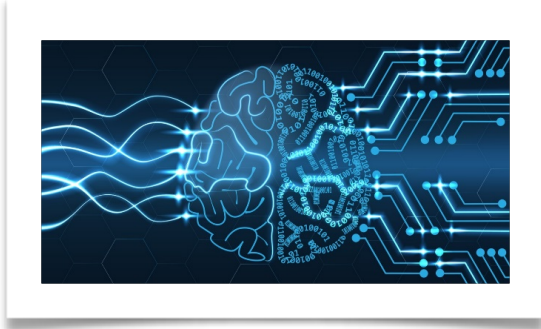
Yasa, şirketlerin bir kişinin verilerini satmasını veya paylaşmasını engelliyor ve verilerin kimliksizleştirilmesi için çaba göstermelerini zorunlu kılıyor. Ayrıca, tüketicilere hangi bilgilerin toplandığını bilme ve bu bilgileri silme hakkı veriyor.

Tasariya ortak sponsor olan Neurorights Foundation'ın genel danışmanı Jared Genser, yaptığı açıklamada, "Bu yeni yasa, tüketicilerin hayatlarını daha güvenli hale getirecek ve hızla büyüyen nöroteknoloji endüstrisine, tüketicilerin zihinsel gizliliği için sağlam korumalar sağlamaları konusunda net bir mesaj verecek" dedi.

Genser, California yasasının, dünyanın dört bir yanındaki bireylerin zihinsel gizliliğini koruyan ulusal ve uluslararası yasalara zemin hazırlayacağını umuyor.

California, başlamak için iyi bir yer—eyalet birçok nöroteknoloji şirketine ev sahipliği yapıyor, bu nedenle tasarımın etkilerinin buradan yayılma ihtimali yüksek.

Duke Üniversitesi'nden hukuk etiği uzmanı Nita Farahany'e göre "sinirsel olmayan bilgi" ifadesinin anlamı belirsiz. Farahany, LinkedIn'de yaptığı bir paylaşımda, "Yasanın dili, bir kişinin beyninden toplanan ham verilerin koruma altında olabileceğini, ancak çıkarımların veya sonuçların—gizlilik risklerinin en fazla olduğu noktalar—koruma altında olmayabileceğini öne sürüyor," şeklinde yazdı.



Uzmanlar tarafından sinirsel verilerin tanımının genişletilmesi ve "bilişsel biyometrikler" olarak adlandırılan yeni bir kategori açılması öneriliyor. Bu kategori, beyin verilerinin yanı sıra fizyolojik ve davranışsal bilgileri de içerebilir, yani, biyosensörler aracılığıyla toplanan ve bir kişinin zihinsel durumunu ortaya çıkarabilecek hemen hemen her şey.

Sonuçta, nasıl hissettiğimizi ele veren tek şey sadece beyin aktivitelerimiz değil. Örneğin, kalp atış hızının artışı heyecanı ya da stresi gösterebilir. Göz izleme cihazları, yapacağımız bir seçim ya da tercih edeceğimiz bir ürünü ortaya çıkarabilir. Bu tür veriler, son derece özel bilgileri açığa çıkarmak için hâlihazırda kullanılıyor. Son araştırmalar, gönüllülerin cinsel yönelimlerini veya eğlence amaçlı uyuşturucu kullanıp kullanmadıklarını

EEG verileriyle tahmin etmeyi başardı. Ayrıca göz izleme cihazları kullanılarak kişilik özellikleri çıkarımları yapıldı.

Tüm bunlar göz önüne alındığında, zihinsel gizliliğin korunması konusunda doğru adımların atılması hayati öneme sahip.

KAYNAKÇA :

<https://www.technologyreview.com/2024/10/04/1104972/law-california-protects-brain-data-doesnt-go-far-enough/>

POS CİHAZLARINDAKİ SATIŞ DIŞI İŞLEMLERDE VERGİSEL BOYUT

AV. OĞUZHAN SEYMEN

İşbu yazıda; Katma Değer Vergisi gelir vergisi Vergi Usul Kanunu ve e-fatura e-arşiv fatura takibi açılarından değerlendirilecektir.



* POS cihazlarından yapılan satışların yanlış veya kötüye kullanıldığında ne gibi uyumsuzluklar doğacağı

* ve bu uyumsuzlukların çözümünün ne olacağı belirtilecektir.

1- POS cihazından satış dışı işlem yapmak ne demektir?

POS[Point Of Sale-Satış Noktası] cihazından mal ve hizmet satışları ile taksitli satışlar ve sanal POS işlemleri yapılmaktadır.

Bu belirtilen işlemlerin haricindeki;

* nakit avans ve paraya çevirme işlemi

* sahte veya gerçek dışı işlemler

* vergi kaçırma amaçlı işlemleri

* ve bankacılık düzenlemelerine aykırı işlemler,

POS cihazında yapılamayan ve kısıtlanan işlemlerdir.

Belirtilen bu harici tüm işlemler; satış dışı işlem olarak geçip MASAK, BDDK ve

Gelir İdaresi Başkanlığı kurmaylarının denetiminden geçmektedir.

Bu kapsamda da mesela;

- Sahte satış yapıp tutarı nakit olarak müşteriye geri vermek ve bu eylemin vergi kaçakçılığı - kara para aklama kapsamına girebileceği,

- Sırf banka kredisi çekebilmek ve komisyon elde edebilmek için gerçek olmayan malın hizmetin satışı varmış gibi göstermek

* ve bunun POS cihazına ilişkin sözleşmenin iptaline ve POS cihazının bloke edilmesine sebep olabileceği,

- POS cihaz üzerinden yapılan satışlarda fatura ve fiş kesilmemesinin ve

- * kayıt dışı ekonomi ile mücadele kapsamında POS işlemleri ile fatura kayıtlarını çapraz kontrol edilmesine neden olunmasının her biri POS cihazındaki satış dışı işlemdir

Dolayısıyla POS cihazları;

- nakit çekme,
- sahte satış vergi kaçırma ve/veya
- yasa dışı finansal işlemler için kullanılır ise

Sadece POS cihazı kullanan satıcı değil

Aynı zamanda bankalar da Gelir İdaresi Başkanlığı ve MASAK tarafından son derece ciddi yaptırımlara tabi tutulabilir.

2- Satış dışı işlemler, vergisel boyut açısından nasıl değerlendiriliyor?

Katma değer vergisi bakımından;

Sahte iade veya iptal işlemleri yapıldığında işletmeler, gerçek

ödemesi gereken KDV'yi azaltabilir ve bu vergi kaybı yaratır.

Ayrıca kayıt dışı satış yapıp KDV tahsil edilmesine rağmen işlem beyannamesine dahil edilmezse yine vergi kaybı yaratılır.

Gelir vergisi ve kurumlar vergisi açısından da;

POS işlemleri işletmenin bu vergilerinin matrahını etkilemektedir.

Belirtilen sahte iadeler ve iptallerde gelir düşük gösterilirse vergi müfettişleri işletmenin beyan ettiği gelir ile POS hareketlerini karşılaştıracak ve beyan dışı kazanç varsa, gerekli yaptırımın uygulanmasını sağlayacaktır.

Vergi Usul Kanunu açısından E-fatura/ e-arşiv fatura sistemleri ile POS işlemleri arasında uyumsuzluk olmamalıdır.

Mesela POS cihazındaki tahsil edilen tutar e- faturaya yansıtılmalıdır.

İptal ve iade işlemi varsa ve fatura düzenlediyse bu fatura iptal edilmelidir.

Denetimlerde POS hareketleriyle fatura kayıtları çapraz kontrol edildiğinde, yüksek iptal ve yüksek iade yapan işletmeler riskli mükellef olarak incelemeye tabi tutulabilir.

3-Uyumsuzluklar özetle nelerdir ve ne gibi çözümler önerilmektedir?

- POS cihazındaki tahsil edilen tutarların faturalara yansıtılmaması,
- Sahte iadeler ve sahte iptallerle haksız KDV iadeleri alınması
- POS işlemleri ile beyan edilen gelir arasında fark oluşması
- ve POS işlemleri dâhil muhasebe kayıtlarının düzenli tutulmamasından kaynaklı uyumsuzluklar,

Vergi incelemelerine tabi tutulabilir, cezalı tarhiyatlara sebep olabilir.



Çözüm önerisi olarak;

Vergi dairesi ile mükellef arasında uzlaşma sağlanması,

Vergi kaçakçılığı ve kara para aklama şüphesi halinde Gelir İdaresi Başkanlığı ve MASAK denetimleri kapsamında soruşturmalar başlatılması,

Ayrıca mükelleflerin haksız tarih edilen cezalar ve ek vergilere itiraz için vergi mahkemesine başvurusu önerilmektedir.

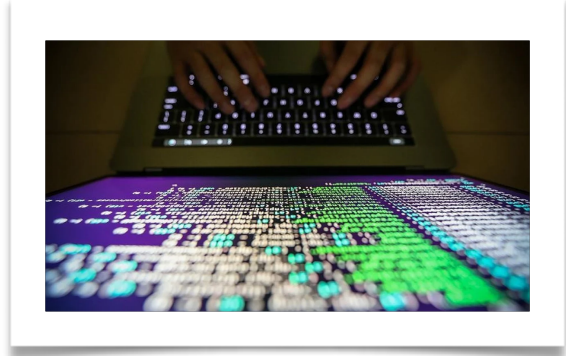
TÜRKİYE'DE SİBER GÜVENLİK VE YENİ KANUN DÜZENLEMELERİ

AV. AHMET KALKAN

Dijital çağın getirdiği olanaklar, hayatımızı kolaylaştırırken beraberinde birçok risk ve tehdit de doğurmuştur. Özellikle siber güvenlik, ülkelerin ulusal güvenlik politikalarının mihenk taşlarından biri haline gelmiştir. Türkiye de bu doğrultuda siber tehditlere karşı önlem almak amacıyla çeşitli adımlar atmış en son olarak da Türkiye Büyük Millet Meclisinde kabul edilen Siber Güvenlik Kanunu ile bu süreci ileri seviyeye taşımıştır.

Türkiye'de siber güvenlik ile ilgili ilk kapsamlı düzenlemeler, 2000'li yılların başında başlamıştır. 2007 yılında yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, internet ortamındaki suçların önlenmesi amacıyla oluşturulmuş olsa da zamanla günümüz siber tehditlerine karşı yetersiz kaldığı görülmüştür.

2012 yılında Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi kurulmuş ve kamu kurumlarının siber güvenliğini sağlamaya yönelik çalışmalar başlatılmıştır. 2016 yılında çıkarılan Kişisel Verileri Koruma Kanunu'da veri güvenliğini sağlamaya yönelik önemli bir adım olmuştur. Ancak tüm bu düzenlemelere rağmen Türkiye'nin siber güvenlik alanında uluslararası standartları yakalaması için daha kapsamlı bir yasal çerçeveye ihtiyaç duyuluyordu. İşte bu bağlamda yeni kabul edilen Siber Güvenlik Kanunu büyük önem taşımaktadır.



TBMM'de kabul edilen yeni Siber Güvenlik Kanunu'nun 13 maddesi, Türkiye'nin siber güvenlik alanındaki savunmasını güçlendirmeyi hedeflemektedir. Bu yeni düzenlemeyle birlikte öncelikli olarak Siber Güvenlik Kurulu oluşturulması planlanmaktadır. Bu kurul; Cumhurbaşkanı, Cumhurbaşkanı Yardımcısı, ilgili bakanlar, Milli Güvenlik Kurulu Genel Sekreteri, Milli İstihbarat Teşkilatı Başkanı, Savunma Sanayi Başkanı ve Siber Güvenlik Başkanı'ndan oluşacaktır. Kurul, ulusal güvenlik açısından kritik kabul edilen bilişim altyapılarının korunmasını sağlayacak ve siber olaylara hızlı müdahale edebilmek için kararlar alacaktır.

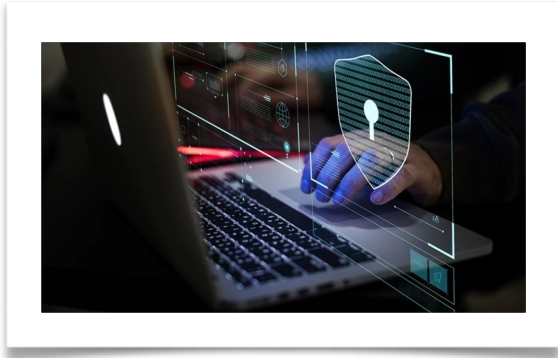
Ayrıca, kanunun önemli maddelerinden biri de yerli ve milli siber güvenlik ürünlerinin tercih edilmesi yönündedir. Türkiye, özellikle kritik altyapılarda dışa bağımlılığı en aza indirmek için bu düzenleme ile kendi yazılım ve donanımlarını geliştirmeye odaklanacaktır. Böylece, olası siber saldırılara karşı daha güçlü ve bağımsız bir savunma sistemi oluşturulması hedeflenmektedir.

Bunun yanı sıra, siber saldırıların önlenmesine yönelik önleyici tedbirlerin artırılması sağlanacaktır. Kamu ve özel sektörde faaliyet gösteren kuruluşlara yönelik siber güvenlik standartları

belirlenerek bu standartlara uyulmaması durumunda yaptırımlar uygulanacaktır. Özellikle kritik sektörler olarak kabul edilen finans, enerji, telekomünikasyon ve ulaşım alanlarında güvenlik seviyesinin artırılması planlanmaktadır.

Yeni yasa teklifi bazı çevreler tarafından eleştirilerle karşılandı. Özellikle, kişisel verilerin korunması, ifade özgürlüğü ve özel hayatın gizliliği açısından endişeler dile getirildi. Kanun teklifinde yer alan ve Siber Güvenlik Kurulu Başkanı'na geniş yetkiler tanıyan 8. madde, gelen eleştiriler üzerine tekliften çıkarıldı. Bu maddenin, bireylerin özel verilerine erişimi kolaylaştırabileceği ve hukuki güvenceleri zayıflatabileceği yönünde görüşler dile getirilmişti.

Ayrıca, siber güvenlik denetim süreçlerinin nasıl yürütüleceği konusunda belirsizlikler olduğu ve daha açık düzenlemelere ihtiyaç duyulduğu belirtilmiştir. Türkiye'de faaliyet gösteren uluslararası şirketler de yeni düzenlemelerin kendileri için ek yükümlülükler doğurabileceği konusunda endişelerini ifade etmişlerdir.



Yeni kanunun kabul edilmesiyle birlikte Türkiye'nin siber güvenlik alanında daha güçlü bir yapı kuracağı beklenmektedir. Özellikle yerli siber güvenlik şirketlerine teşvikler sağlanarak ülke içindeki siber güvenlik ekosisteminin güçlendirilmesi hedeflenmektedir.

Ayrıca, uluslararası iş birliklerinin artırılması gerekliliği ön plana çıkmaktadır. Siber saldırılar küresel bir tehdit olduğundan,

Türkiye'nin NATO ve diğer uluslararası kuruluşlarla iş birliğini güçlendirmesi kaçınılmazdır. Bu kapsamda, Türkiye'nin siber savunma stratejisini daha geniş bir çerçevede ele alarak uluslararası standartlarla uyumlu hale getirmesi gerekmektedir.

Bireyler açısından bakıldığında, vatandaşların siber güvenlik farkındalığının artırılması ve bilgi güvenliği eğitimlerinin yaygınlaştırılması önem arz etmektedir. Kanunun sadece teknik düzenlemeler getirmekle kalmayıp, toplumun bilinçlenmesini sağlayacak adımlar atması gerektiği de unutulmamalıdır.

Sonuç olarak, Türkiye'de siber güvenlik konusunda uzun zamandır beklenen köklü düzenlemeler hayata geçirilmeye başlanmıştır. Yeni kabul edilen Siber Güvenlik Kanunu, ulusal güvenliği güçlendirme, yerli teknolojileri teşvik etme ve kamu-özel sektör iş birliğini artırma açısından önemli bir dönüm noktasıdır. Ancak, bu düzenlemelerin başarılı olabilmesi için uygulamada şeffaf, denetlenebilir ve insan haklarına saygılı bir yaklaşım benimsenmesi gerekmektedir.