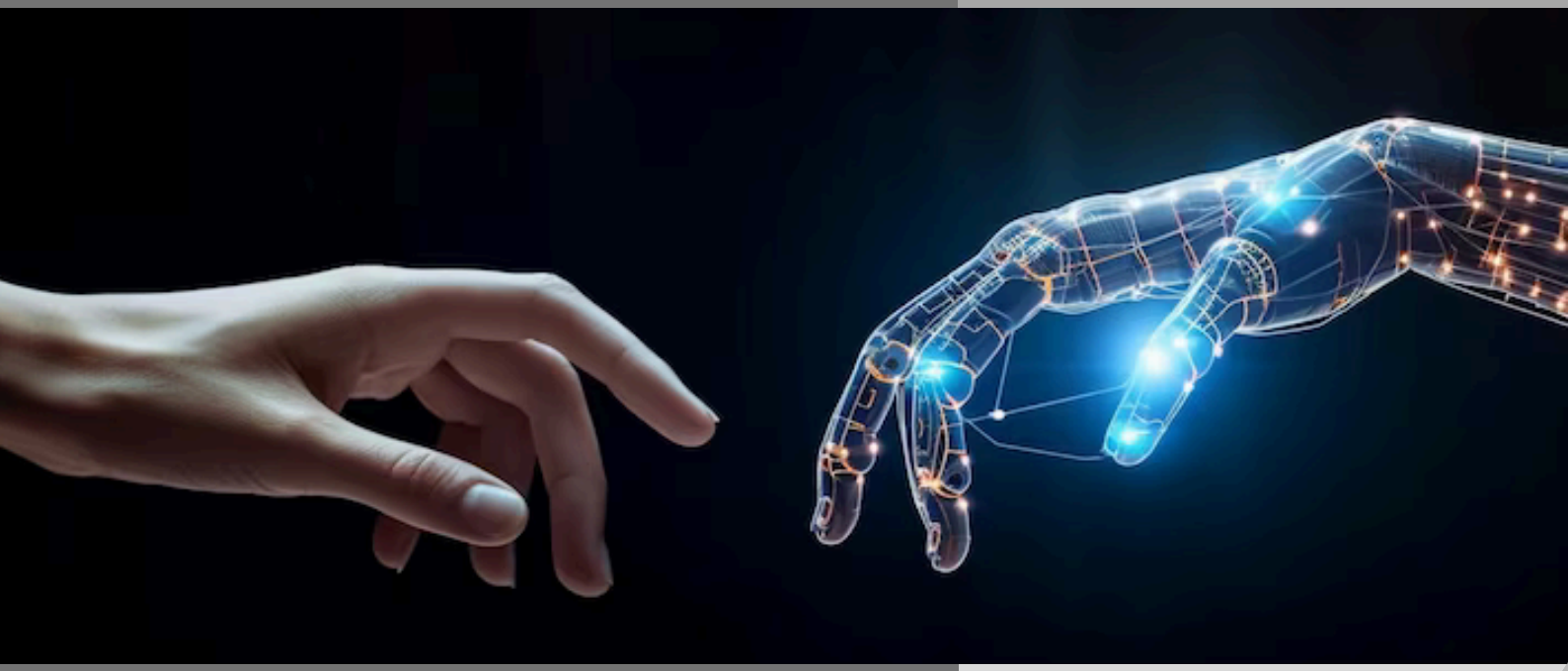
EYLÜL-ARALIK 2025 | SAYI 20

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.

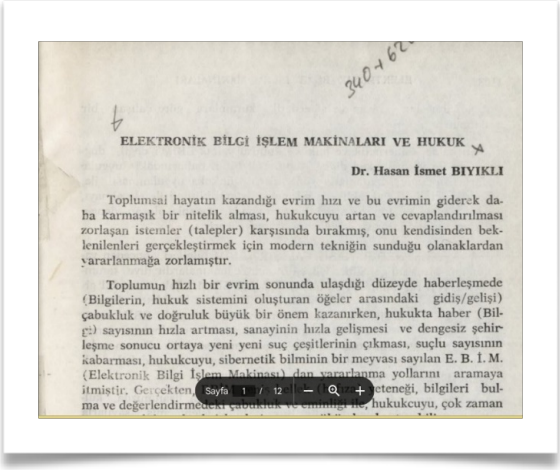
Bilişim hukuku alanında meslektaşlarımızın sizler için hazırladığı makaleleri, haberleri, dizi, film ve kitap önerilerini ve daha birçok içeriği her ay bültenimizden takip edebilirsiniz.

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

Saygılarımızla.

ELEKTRONİK BİLGİ İŞLEM MAKİNALARI MAKALESİ İLE UYAP'IN 1970'LERDE ÖNGÖRÜLMESİ

Av. OĞUZHAN SEYMEN



ELEKTRONİK BİLGİ İŞLEM MAKİNALARI VE HUKUK

Dr. Hasan İsmet BIYIKLI

Toplumsal hayatın kazandığı evrim hızı ve bu evrimin giderek daha karmaşık bir nitelik alması, hukukcuyu artan ve cevaplandırılması zorlaşan istemler (talepler) karşısında bırakmış, onu kendisinden beklenilenleri gerçekleştirmek için modern tekniğin sunduğu olanaklardan yararlanmağa zorlamıştır.

Toplumun hızlı bir evrim sonunda ulaşdığı düzeyde haberleşmede (Bilgilerin, hukuk sistemini oluşturan öğeler arasındaki gidiş/gelişi) çabukluk ve doğruluk büyük bir önem kazanırken, hukukta haber (Bilgi) sayısının hızla artması, sanayinin hızla gelişmesi ve dengesiz şehirleşme sonucu ortaya yeni yeni suç çeşitlerinin çıkması, suçlu sayısının kabarması, hukukcuyu, sibernetik bilminin bir meyvası sayılan E. B. İ. M. (Elektronik Bilgi İşlem Makinası) dan yararlanma yollarını aramaya itmiştir. Gerçekten, [illegible] yeteneği, bilgileri bulma ve değerlendirmedeki çabukluk ve [illegible] hukukcuyu, çok zaman

"Elektronik bilgi işlem makinaları(EBİM) ve hukuk" başlıklı makalesi ile Dr. Hasan İsmet Bıyıklı; adeta internetin ve kişisel bilgisayarların hayal bile edilemediği bir dönemde günümüz hukuk teknolojilerini ta 1970'li yıllarda, şaşırtıcı bir öngörüyle ele almıştır.

1-Bu makale neden önemli?

Günümüzün hukuki veri tabanları" işlevine bu makalede yazar ; "hukuk dökümanlarının saklanması ve değerlendirilmesi" alt başlığında, "metinlerin tam metin veya özet olarak kaydedilmesinin" yanı sıra tanımlamalarda önemli kavramlara değinmiştir:

1- "Gürültü" [ilgisiz sonuç] ve
2- "Suskunluk" [ilgili sonucun çıkmaması]

Bu kavramlar EBİM'e bilgiler verilmesi gerektiği, programların EBİM'e neler yapabileceğini belirtiyor olduğu, dolayısıyla "kendisine ilgili bilgileri nasıl ve hangi sırayla işleyeceğini gösteren emir ve talimatlar listesi verilmezse EBIM'in anlamsız cevabına ve susmasına yol açılacağı" anlamına gelir.

Adliyenin yan hizmetleri başlığı altında da aşağıda açıklanacak olan ; "Merkezi adli sicil hizmetleri, trafik ve araç biriklerinin tek bir veri tabanında toplanması ve mahkum dosyalarının merkezi sistemle takibi" gibi ufuk açıcı fikirler vardır.

Bu fikirlerle makalede inanılmaz şekilde ulusal yargı ağı projesi UYAP'ın temelleri atılmıştır...

Öte yandan "ileriye dönük araştırmalar" başlığı ile "yasa tasarılarının olası etkilerinin hesaplanması, yasalar arasındaki ilişkilerin tespiti ve kurulacak bilgi bankalarının, kişi özel hayatının gizliliğini ihlal edebilecek olması tehlikesine" dikkat çekilmiştir.

Böylelikle hem veriye dayalı kanun yaptırımı hem de kişisel verilerin korunması gibi kritik konular , "ta 1973 tarihli Adalet dergisi arşivinde dahi", öngörülebilmiştir.

2- Makalede temel olarak hangi başlıklar neden incelenmiştir?

a]Makalede "sibernetik" kelimesinin meyvesinin, EBİM olduğu, toplumsal hayatın evrim hızı ve karmaşıklığının önemi, bilginin çabukluğu ve doğruluğunun mühimliği ele alınmıştır.

Bu düzlemde de "hukukta haber sayısındaki artışın, sanayinin hızlı gelişiminin, dengesiz şehirleşmenin, yeni suç çeşitlerinin ve suçlu sayısının kabarmasının" etkilerine dikkat çekilmiştir.

b]EBİM'in ne olduğu, nasıl işlediği, hukuk alanında ne amaçlarla - nasıl kullanıldığına da değinilmiştir.

Makalede "EBİM'in, yön-eylem araştırmaları, oyun kuramı, sistem anlayışı ve program kuramı metotlarıyla elde edilen bilgilerin, verilerin büyük bir çabuklukla ve yanılgıya yer vermeksizin değerlendirilmesine yarayan ve sibernetik kuramlara göre çalışan makineler olduğu" belirtilmiştir.

c]"Sibernetik ve hukuk" demek sadece EBİM demek olmayıp, "doğrulukları - yararlılıkları ve diğer toplum bilimleriyle ilişkisi açıkça saptanarak, matematik yöntemlerinin hukuka uygulanmasının sağlanması" demektir.

"Sibernetik ve hukuk", işlevsel olarak "hukuk sistemindeki aksaklıkları görmeyi, sistem bütün olarak ele almayı ve hukuk sistemi ile toplum sistemleri arasında zamanla oluşan dengesizliklerin giderilmesi" yollarını aramıştır.

d]EBİM'in nasıl çalıştığı noktasında, "önceden yapılmış bir program gereğince işleyebilen otomatik makine" olduğu söylenebilir.

Burada "otomatikten" kasıt , "EBİM'lerin, sistemi harekete geçirdikten sonra, makinenin insan müdahalesi olmadan bilgi işleyebilmesi" , demektir

Aslında EBİM, insana yardım ile "elektrik enerjisi ile insanın bellek gücü - düşünme kapasitesi - düşünme yeteneğinin artırılmasına" yarar.

3- EBİM'in hangi üniteler ile ilkel olarak nasıl çalıştığı hakkında neler söylenebilir?

EBİM'in, giriş /merkez / çıkış şeklinde 3 ünitesi vardır.

Giriş; delikli kart ve manyetik bant olarak EBİM'e bilgi verilmesini sağlıyor.

Merkez'e; ana bellek ve işlem üniteleri ile işlenmeden önce ve sonra bilgileri saklamaya yarayan depo diyebiliriz.

Merkeze bağlı; "işleme ünitelerindeki kontrol ve aritmetik mantık" kısımları kendisine ulaştırılan bilgileri , "direktifler dairesinde toplar- çıkarır -böler -karşılaştırır". Dolayısıyla belirli bir konuyu ilgilendiren belgeleri bir araya toplayan önemli bir ünitedir.

Çıkış ünitesi; bana müzekkere yazımını Hatta Yapay Zeka botlarının ilk halini andırıyor.

Çünkü işlenmiş bilgilerin, bize iletildiği üniteler olup, araçlara bağlı teleks-terminal ve TV ekranları gibi sonuçların, EBİM'in bulunduğu merkezlerden uzağa aktarılmasını sağlıyor.

Çıkış ünitesi öyle bir ünitedir ki niceliksel işlemleri niteliksel işleme çevirir.

Mesela matematiksel işlemleri ; ana bellekte aranmış- bulunmuş olan hukuk belgelerini, bizim anlayacağımız dilde yazma yeteneği bile bulunur.

Ozetle fonksiyonel olarak EBIM için söyleyebiliriz ki tek başına hareket edemez ancak otomatik olarak veri işlerler.

Kendisine verilmiş bilgileri, önceden belleklerine kaydedilmiş program gereğince, otomatik olarak başka hiçbir müdahaleye gerek olmaksızın işleyebilirler.[Bu yönü, DAO'lara-merkeziyetsiz otonom organizasyona benzetilebilir.]

4- Hukukumuzda EBİM'den nasıl yararlanıyoruz?

Makale, hukuk belgelerinin bilgisayar belleğine kaydedilmesi ve taranması için iki ana sistemden bahseder:

ilki Tam Metin Sistemi (Natural Language)'dir.

Yasaların ve kararların hiçbir kısaltma yapılmadan belleğe aktarılmasıdır.

Bilginin değerini koruması açısından avantajlıdır ancak çok yer kaplaması ve arama süreçlerinin yavaş olması (o dönemin teknolojisiyle) dezavantajdır.

2ncisi; Özetleme Sistemi (Documentary Language)'dir.

Bilgilerin özetlenerek kaydedilmesidir.
Yer ve zaman tasarrufu sağlar ancak özetleyen kişinin tarafsızlığını yitirmesi veya önemli detayları atlaması gibi riskler taşır.

5- EBİM; Adalet Sistemimizin başka neresinde kullanılıyor?

Bilgisayar sistemlerinin adalet mekanizmasında aşağıda belirttiğim alanlarda devrim yaratmakta olduğunu söyleyebilirim:

ilki Adli Takip ve Polis Hizmetleri'dir
Suçluların kaydı, sabıka kayıtları, parmak izlerinin saklanması ve gerektiğinde ekranlara (televizyon görüntüsü gibi) hızlıca getirilmesi, sağlanır.

2ncisi; Trafik Denetimidir. Araçların plaka, motor numarası ve sahip bilgilerinin dijital bir "bilgi bankasında" tutularak anlık sorgulanabilmesi, sağlanır.

3'üncüsü; Ceza İnfaz Kurumlarıdır. Mahkumların şahsi dosyalarının takibi ve ıslah süreçlerinin (tretman) dijitalleşmesi, sağlanmaktadır.

6- Hiç mi sorun ile karşılaşılmıyor EBİM'de ve teknik hiç mi aksaklık yok? Ya da ne gibileri olası?

Bir defa Dil ve Mantık Sorunu var.

Hukuk dilindeki eş anlamlı kelimelerin bilgisayar tarafından yanlış algılanması ("gürültü" denilen ilgisiz cevapların çıkması), söz konusu,demiştik.

Bunun bir de Maliyeti var.

EBİM sistemlerinin çok pahalı olması nedeniyle kurumların (barolar, üniversiteler, bakanlık) ortak girişim yapması önerilmektedir.

Güncellik: ister.
Mevzuat veya içtihat değiştiğinde eski bilgilerin silinip yenilerinin anında sisteme girilmesinin zorunluluğu vardır.

7- Peki işin özünden ne anlıyoruz ve makalede ne gibi çözümler öneriliyor?

Yazar makalesinde, modern toplumda iş hacmi artarken adaletin "ilkel yöntemlerle" devam edemeyeceğini vurgular. Çözüm olarak önerileri elbette vardır.

Hukukçu-Uzman İş Birliğinden söz ediliyor. Sistemler kurulmadan önce hukukçular ile bilgisayar uzmanlarının birlikte çalışması gerekmekte.

Eğitim de şart. Hukuk fakültelerinde "informatik" (bilgisayar bilimleri) derslerinin verilmesinin kaçınılmaz bir zorunluluk olduğu belirtiliyor.

Kurumsallaşmak da lazım. Adalet Bakanlığı bünyesinde veya bağımsız bir "İnformatik Müdürlüğü" kurulması gerektiği ifade ediliyor.

Demem o ki bu Tarihi Makale; bilgisayarların henüz "delikli kartlarla" çalıştığı ve saniyenin 1/1000'i hızındaki işlemlerin bile büyük başarı sayıldığı bir dönemi yansıtması açısından tarihsel bir öneme sahip.

8- Bu makale, bana bazen bir bilim kurgu filmini 1970'lerde izletmiş gibi geliyor. Çünkü şu an o bilim kurgu gerçeğe dönüşmüş durumda:

Türkiye'de dijital adaletin koridorları UYAP gibi sistemlerle titreşirken,

Ankara'da Bakanlık'taki yetkililer yapay zekâ destekli dava tasnifi ve içtihat analiz süreçlerinin hukukun hızını artırma hedefiyle geliştirildiğini vurguluyor…

Bakanlık , bu sistemlerin hâkim iradesini ortadan kaldırmayacağını, yalnızca iş yükünü ve nesnelliği güçlendireceği belirtiliyor.

("Her nasılsa duruşmalar halen yavaş, kararlar halen geç veriliyor. Belki de istinafı ortadan kaldırsak ve karar yazma süresi getirsek , bu yavaşlık gerçek anlamda hızlanmaya dönüşebilirdi.")

Aynı zamanda Adalet Bakanı'nın açıklamasında da belirtildiği gibi, dijitalleşme ve yapay zekâ kullanımı, hak ve özgürlükleri zedelemeden veri güvenliği ve hukuk ilkeleri kapsamında yürütülmesi gerektiği açıklandı; Türkiye bu dönüşümü hukuki ve etik temellerle inşa etmeye kararlı olduğunu söylüyor. (Tech and Justice, TRT Haber). Ben de acaba diyorum.

Buna paralel olarak, Türkiye Bilimler Akademisi'nin uluslararası sempozyumunda araştırmacılar, dijital hukukun yalnızca teknoloji getiren yenilikleri düzenlemekle kalmayıp, aynı zamanda bireylerin mahremiyetini, veri egemenliğini ve insan merkezli yaklaşımı korumak için hukukun rolünü yeniden tanımlaması gerektiğini vurguladı; çünkü algoritmalarla şekillenen dijital dünyalar, ortak adalet anlayışımızı zayıflatabilir, diyorlar…

KVKK gibi kurumlar da düzenlenen etkinliklerde yapay zekâ sistemlerinde kişisel verilerin korunmasının önemi, bireyin sürece itiraz hakları ve şeffaflık ile insan denetimi gibi ilkelerin teknolojiyle yargının dengesi açısından kritik olduğunu hatırlatıyor. (Türkiye Bilimler Akademisi, Kişisel Verileri Koruma Kurumu)

Bu yerel tartışmaların ötesinde, Avrupa'da da dijital hukukun korunması büyük bir gündem maddesi, diyebiliriz.

Avrupa Birliği'nin yapay zekâ alanındaki düzenlemeleri, sistemleri yüksek riskten kabul edilemez riske kadar sınıflandırarak güvenlik, şeffaflık ve insan denetimi gibi standartlar getirmeyi amaçlıyor; bu düzenlemelerin kabulüyle Avrupa, aslında güvenli inovasyonun merkezi olma arayışında.

Dahası, Avrupa konseyi çatısı altında imzalanan uluslararası bir anlaşma, yapay zekânın insan hakları, demokrasi ve hukukun üstünlüğü ile uyumlu şekilde gelişmesini sağlama hedefini benimsiyor — bu, sadece teknolojinin gelişmesi değil, hukukun teknolojiye rehberlik etmesi gerektiğini gösteren küresel bir adım gibi. (Reddit, Vikipedi)

Amerika tarafında da mesele farklı bir tavırla ilerliyor; örneğin ABD Telif Hakları Ofisi, AI tarafından üretilen içeriklerin yalnızca insan katkısı olan kısımlarının telif koruması alabileceğini ilan ederek, yapay zekânın hukuki statüsünü belirginleştirme yönünde net ilkeler koyma çabası içine girmişti. (Reddit)

Ve bütün bu haberlerin, analizlerin ve hukuki tartışmaların ortasında durduğunda fark ediyorsunuz ki;

Teknolojinin hızla dönüştürdüğü hukuk, yalnızca otomasyon değil, şeffaflık, insan hakları, veri koruması ve denetim ilkeleri ile korunabilir.

Çünkü adaletin dijital dünyada ayakta kalması, makine kodlarıyla değil, hukukun insanı merkez alan değerleriyle mümkün olur — bir makinenin çıktısı ile değil, insanın iradesi ve hukukun sunduğu güvenceyle , mümkündür.

9- Makalemizi, teknik-hukuki-felsefik açıdan değerlendirirsek; şöyle toparlayabiliriz:

Ana fikir anlamında, makalede;

elektronik bilgi işlem makinelerinin (bugünkü bilgisayarların) hukuk alanında destekleyici bir araç olarak büyük faydalar sağlayabileceğini, ancak insan yerine geçemeyeceğini,

özellikle yargılama ve karar verme yetkisinin makineye bırakılamayacağını vurgular. EBİM; bilgi toplar, saklar, karşılaştırır ve sonuç üretir, fakat hukuki muhakeme yapamaz, diyebiliriz.

EBİM'in teknik yapısı için ne demiştik:

Makalenin, bilgisayarın temel işleyişini açıkladığını,
Giriş ünitesinde verilerin sisteme girildiği, ana bellekte bilgi ve programların saklandığı, kontrol ünitesinde işlemlerin sırasının ve düzeninin sağlandığı, aritmetik-mantik ünitesinde hesaplama ve karşılaştırma yapıldığı ve nihayet Çıkış ünitesinde sonuçların insana anlaşılır biçimde sunulduğunu, konuştuk.
Önemle vurgulamıştık ki;
EBİM'ler, kendi başına hareket edemez; yalnızca önceden verilmiş program ve bilgilerle çalışır.

10- EBİM' hukukta nasıl işimize yaradı, yarıyor ve yarayacak?

İçtihatların, yasaların ve ilmi görüşlerin saklanması
Hızlı arama ve karşılaştırma yapılabilmesi
Hukukçunun zaman kaybından kurtulması
Daha objektif ve sağlam karar altyapısı İmkanları mevcut.

Makalesinde yazar, bunu ayna–dikiz aynası benzetmesiyle açıklar:

GEÇMİŞİ İYİ GÖRMEK, BUGÜNÜ DAHA GÜVENLİ YÖNETMEYİ SAĞLAR.

İleriye Dönük Araştırmalar noktasında,
Yasaların uygulamada doğuracağı sonuçların önceden hesaplanması
Yasa taslaklarının etkilerinin değerlendirilmesi
Suç politikası gibi alanlarda veriye dayalı yön belirlenmesi
Bakımlarından umut vaad ediyor…

Demek ki EBİM neymiş, yasa koyucuya uyarı ve öngörü aracı olurmuş ama karar merci değilmiş…

11- Yasaları, makaleye göre EBİM ile nasıl uygulamaktayız?

Yazar çok net bir sınır çizer ve der ki; EBİM, muhakeme yeteneğine sahip değildir ve karar veremez.

Ancak ekler; İşçi ücretleri, Memur maaşları, Net, yoruma kapalı düzenlemeler gibi alanlarda otomatik uygulama mümkündür, der.

Bu sürecin, Verilerin insan eliyle toplanması, EBİM'de değerlendirilmesi ve Sonuçların saklanması
şeklinde işlediğini, bunu şematize ederek belirtir.

12- İlk bahsettiklerimize ek olarak "Hukuki ve Politik Sorunlar" yok mudur?

Yazara göre ta o zamandan öngörülmüştür, vardır.

Erken dönemde çok kritik risklere işaret eder. Yasaların dilinin sadeleştirilmesi gereği, Yasalar arası çelişkilerin ortaya çıkması, EBİM'in verdiği sonuçlardan kimin sorumlu olacağı ve EBİM yoluyla

verilen kararların nasıl denetleneceği… kaygı uyandırıyor ama çözümün de teknik olduğu kadar bir hukuk politikası olduğunun altını çiziyor.

13- Adliyenin yan hizmetlerinde makaleye göre EBİM nasıl işimize yaramakta?

Özellikle, Adli sicil hizmetleri, Polis ve trafik kayıtları, İnfaz ve idari işlemler, alanında EBİM'in kaçınılmaz olduğu belirtiliyor.

Merkezi bir sistem sayesinde Hız, Güvenlik, Doğruluk, sağlanabilir.

Ancak uyarı net. Merkezileşme, yanlış ve eksik veriler girildiğinde büyük hak ihlallerine yol açabilir.

14- İşbu yazıda, bu makaleyi inceleyerek size hangi mesaj verildi?

İşbu yazım ile ve makalenin incelenmesiyle sizlere, elektronik bilgi işlem makinelerinin hukuku hızlandıran, düzenleyen ve destekleyen güçlü araçlar olduğunu; ancak hukuki muhakeme, vicdan ve sorumluluk gerektiren alanlarda insanın yerini alamayacağı mesajı verildi.

EBİM, geçmişi daha net görmeyi ve geleceği daha isabetli öngörmeyi sağladığı

fakat karar verme yetkisi makineye devredildiğinde hukuk mekanikleşeceği ve adaletin zedeleneceği,

Bu nedenle UYAP'ın daha 1970'lerde temelinin öngörüldüğü, bununla birlikte teknolojinin hukukun yerine konulmaması gerektiği, hukukun hizmetine konulması gerektiği, izah edildi ve takdirlerinize sunuldu.

KAYNAKÇA:

1. https://www.techandjustice.bsg.ox.ac.uk/research/t%C3%BCrkiye?utm

2. https://www.trthaber.com/haber/gundem/bakan-tunc-turkiyede-hukuk-alanindaki-dijitallesmeyi-derinlestirmekte-kararliyiz-923867.html?utm

3. https://tuba.gov.tr/tr/haberler/akademiden-haberler/yapay-zek-hukuku-sempozyumu-uluslararasi-katilimla-erude-gerceklesti?utm

4. https://www.kvkk.gov.tr/Icerik/8331/Mart-Mayis-2025-Sayi-8-Yapay-Zekaya-Genel-Bakis-?utma

5. https://www.reddit.com/user/ibrahimxcan/comments/1oyjfna/chatgpt_avrupa_birli%C4%9Finin_yapay_zek%C3%A2_yasas%C4%B1/?utm

6. https://en.wikipedia.org/wiki/Framework_Convention_on_Artificial_Intelligence?utm

7. https://www.reddit.com/user/enoumen/comments/1idza8r/ai_daily_news_jan_30_2025_us_copyright_office/?utm

IP BİLGİSİNİN BELİRLENEBİLİRLİĞİ VE FAİLİN TESPİTİNE ETKİSİ

AV. İREM NALBANT

İnternet ortamında gerçekleştirilen fiillerde failin tespiti, çoğu zaman IP adresinin (Internet Protocol Address – İnternet Protokol Adresi) doğru şekilde belirlenmesine bağlıdır. Uygulamada IP adresi, sıklıkla "kişiyi gösteren teknik delil" olarak algılanmakta ise de, bilişim altyapısının işleyişi dikkate alındığında bu kabul her zaman geçerli değildir. Zira IP adresi, doğrudan bir kişiyi değil, yalnızca bir ağ bağlantı noktasını ifade eder.

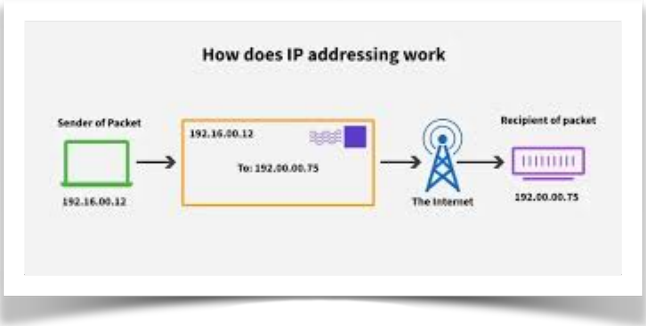
Bu nedenle, IP adresinin tespit edilemediği ya da tespit edilen IP adresinin fiili kullanıcıyla kesin biçimde ilişkilendirilemediği hâllerde failin belirlenmesi teknik olarak mümkün olmayabilir. Aşağıda, IP adresinin neden ve hangi teknik yöntemlerle belirsiz hâle gelebildiği bilişim sistemlerinin çalışma mantığı çerçevesinde incelenecektir.

IP Adresi Kavramı ve Teknik İşlevi

IP adresi, internet üzerinden veri iletimi sağlayan Internet Protocol (IP) sisteminin temel bileşenidir. İnternete bağlanan her cihaz, iletişim kurabilmek için bir IP adresi kullanır. Bu adres, veri paketlerinin (internet üzerinde taşınan bilgi birimleri) hangi noktadan gönderildiğini ve hangi noktaya ulaştırılacağını belirler.

Burada belirtmek gerekir ki İnternet üzerinden gerçekleştirilen hiçbir veri aktarımı tek parça hâlinde yapılmaz. Aksine, iletilmek istenen tüm bilgiler teknik olarak daha küçük parçalara bölünerek gönderilir. Bu küçük parçalara "paket" (packet) adı verilir. Paket kavramı, internet iletişiminin en temel yapı taşlarından biridir ve IP adresine ilişkin tüm teknik tartışmaların merkezinde yer alır.

Bu durumu basit bir benzetmeyle açıklamak mümkündür. Bir kitabın kargo yoluyla gönderildiği düşünülürse, kitabın tek kutuya konması yerine parçalara ayrılarak numaralandırılmış çok sayıda küçük zarf içinde gönderildiği varsayılabilir. Her zarf; kendisini kimin gönderdiğini, kime gideceğini ve gönderinin hangi parçasını taşıdığını belirtir. Öyle ki her zarf gönderilen bilginin küçük bir bölümünü taşırken, aynı zamanda bu bilginin kaynağına ve hedefine ilişkin teknik bilgileri de içerir.



Bir IP paketi teknik olarak iki ana bölümden oluşur. İlk bölüm "başlık" (header) olarak adlandırılır. Bu bölüm, paketin kimlik bilgisi niteliğindedir ve paketin kaynak IP adresini, yani gönderildiği ağ noktasını; hedef IP adresini, yani paketin ulaştırılmak istendiği sunucu veya cihazı; ayrıca paketin sıra numarasını ve hangi iletişim protokolünün kullanıldığını içerir. Fail tespiti bakımından kritik olan tüm bilgiler bu başlık kısmında yer alır. İkinci bölüm ise "veri" (payload) kısmıdır. Bu bölümde gönderilen mesajın, web isteğinin veya dosyanın yalnızca küçük bir parçası bulunur.

Bir kişi internette herhangi bir işlem gerçekleştirdiğinde, örneğin bir web sitesine mesaj gönderdiğinde, bu mesaj teknik olarak paketlere bölünür. Her bir paketin başlığına bir kaynak IP adresi yazılır ve bu paketler internet üzerinden hedef sunucuya iletilir. Hedef sunucu, kendisine ulaşan bu paketleri yeniden birleştirerek işlemi tamamlar. Sunucu kayıtlarında (loglarda) görülen IP adresi, gerçekte paketlerin başlık kısmında yer alan bu kaynak IP bilgisidir.

Özetle paket, internet üzerindeki her işlemin, üzerinde kaynak IP bilgisi bulunan en küçük teknik taşıyıcısıdır. IP adresine ilişkin tüm tespit ve delil tartışmaları, gerçekte bu paketlerin başlık bilgilerinin doğruluğu ve güvenilirliği üzerinden şekillenir.

Tam bu noktada IP protokolü "Bu paketi nereye ulaştırmalıyım?" sorusunu cevaplamak üzere tasarlanmıştır, teknik olarak posta sistemi mantığıyla çalışır. Protokol (postacı) yalnızca alıcı adresine bakar ve zarfı (veriyi) oraya ulaştırır. Bu işlemi yaparken adresin gerçekten paketi gönderen cihaza ait olup olmadığını kontrol etmez yani IP protokolünün merkezi bir doğrulama sistemi yoktur. Eğer sistem kaynak IP doğrulaması yapmaya kalkarsa internet trafiği aşırı yavaşlayacaktır ve günümüzde internet hızı ve internetteki veri akışı yükü da düşünüldüğünde böyle bir sistemin varlığı ölçeklenemez olurdu.

IP protokolü ağdaki cihazların kaynak adresi doğru yazacağını varsayar. Bu teknik bir güven varsayımıdır, hukuki veya güvenlik temelli bir güven değildir. Bu durum, kötü niyetli kişiler tarafından istismar edilebilmektedir.

Protokolün bu eksikliği zamanla fark edilmiş ve sonradan şifreleme veya güvenlik duvarı gibi ek çözümler geliştirilmiştir. Ancak Bu çözümler IP'nin kendisi değildir; IP'nin üzerine eklenmiş ayrı güvenlik katmanlarıdır. Dolayısıyla bu katmanların olmadığı yahut yetersiz kaldığı durumların var olabileceği, sistemin kendi güvenliğinin mevcut olmadığı gözetilmelidir.

IP Adresinin Belirsizleşmesine Yol Açan Teknik Yöntem Örnekleri

Teknik açıdan şu hususun altı özellikle çizilmelidir: Sunucular kişiyi veya cihazı doğrudan görmez; yalnızca kendilerine ulaşan paketi ve bu paket üzerindeki teknik bilgileri görür. Eğer paket üzerinde yer alan kaynak IP adresi sahte ise, başkasına aitse veya aynı IP adresi birden fazla kişi tarafından kullanılıyorsa, bu durumda yalnızca paket başlıklarına dayanarak belirli bir kişiye ulaşmak teknik olarak güvenilir bir sonuç üretmez. Bu teknik gerçeklik, IP adresine dayalı delillerin hukuki değerlendirilmesinde dikkate alınması gereken temel noktayı oluşturur. Bu açıdan IP protokolüne yapılabilecek bazı müdahaleler aşağıda incelenmiştir:

A. IP Spoofing (IP Sahteciliği)

IP Spoofing, gönderilen IP paketlerinde yer alan kaynak IP adresinin, gerçek adres yerine bilerek farklı bir adresle değiştirilmesi işlemidir[3]. Bu yöntemde hedef sistem, paketin geldiği kaynağı yanlış algılar. Yukarıda da bahsettiğimiz gibi IP protokolü ağdaki cihazların kaynak adresi doğru yazacağını varsayacağından IP spoofing, bu güven varsayımının kötüye kullanılmasıdır.

Örneğin bir kişi, kendi IP adresi yerine başka bir ülkeye veya kuruma ait bir IP adresini kullanarak paket gönderdiğinde, hedef sistem işlemi o sahte IP adresine atfeder. Bu yöntemde IP adresi mevcut olsa dahi IP ile fail arasındaki bağ kopmuştur.

B. Proxy ve SOCKS Sunucularının Kullanımı

1. Proxy (Vekil Sunucu)

Proxy sunucular, kullanıcı ile hedef sistem arasında aracı olarak çalışan sistemlerdir. Kullanıcı, hedef siteye doğrudan bağlanmaz; bağlantı proxy sunucu üzerinden gerçekleştirilir. Bu durumda hedef sistem, yalnızca proxy sunucunun IP adresini görür ve kullanıcının gerçek IP adresi gizlenmiş olur. Proxy kullanımı özellikle IP adresinin başka bir ülke veya kurum üzerinden görünmesi, yani failin tespitinin üçüncü bir hizmet sağlayıcıya bağlı hâle gelmesi sonucunu doğurur.

2. SOCKS Proxy

SOCKS, web trafiğiyle sınırlı olmayan, daha genel bir yönlendirme protokolüdür. SOCKS proxy kullanıldığında da hedef sistem, gerçek IP yerine SOCKS sunucusunun IP adresini kaydeder.

Önemle belirtmek gerekir ki SOCKS sistemleri çoğu zaman trafiği şifrelemez; ancak IP adresini maskeleme konusunda son derece etkilidir.

C. VPN (Virtual Private Network – Sanal Özel Ağ)

VPN sistemlerinde kullanıcı trafiği, VPN sunucusuna kadar şifreli bir tünel üzerinden taşınır. Hedef sistem, kullanıcının gerçek IP adresini değil, VPN sunucusunun IP adresini görür.

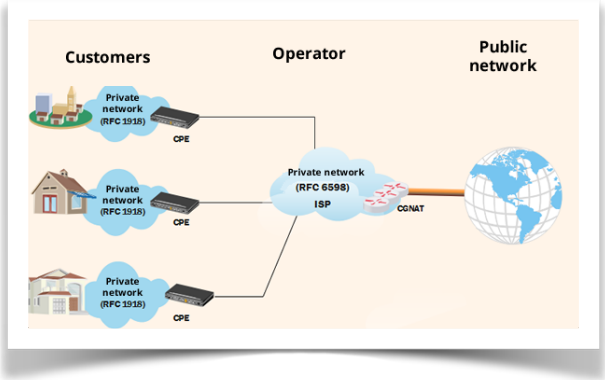
VPN kullanımı, IP adresinin gerçek kullanıcıyla ilişkilendirilmesini ciddi ölçüde zorlaştırır. Her ne kadar VPN ve Proxy yöntemleri benzer görünse de proxy hukuki hata üretme potansiyeli daha yüksek yöntemlerdendir. VPN kullanımının trafik deseninden, şifreleme yapısından, bilinen VPN IP havuzlarından tespit edilme ihtimali daha yüksekken proxy kullanımı ise çoğu zaman standart HTTP/HTTPS trafiği gibi görünür ve bir gizleme yöntemi olarak algılanmayabilir.

D. IP Paketlerinin Düzenlenmesi ve NAT Mekanizması

IP adresinin belirsizleşmesine yol açan bir diğer unsur, Network Address Translation (NAT – Ağ Adres Çevirisi) sistemidir. NAT, birden fazla cihazın internete tek bir genel IP adresi üzerinden çıkmasını sağlar. Bir ev veya ofis ağında onlarca cihaz bulunmasına rağmen, dış dünyaya karşı tüm bağlantılar aynı IP adresinden yapılmış gibi görünür. Bu durumda IP adresi tespit edilse dahi bu IP'nin hangi cihaz veya kişi tarafından kullanıldığı teknik olarak ayırt edilemeyebilir.

Günümüzde dünya çapında mobil operatörler tarafından NAT yöntemi yaygın biçimde kullanılmaktadır. Bu durum Türkiye'deki GSM operatörleri (özellikle Turkcell ve Türk Telekom) açısından da geçerlidir. Böylece Türkiye'de de mobil internet kullanıcılarının gerçek IPv4 adresine ulaşılmasının zor hale geldiği açıktır zira birden çok abone aynı public IP adresini paylaşabilir ve doğrudan kişiye özgü bir IP eşleşmesi teknik olarak mümkün olmayabilir.

Teknik olarak mobil operatörler, IPv4 adreslerinin sayısının sınırlı olması nedeniyle her cihaza doğrudan tekil ve sürekli bir public (genel) IP adresi atamak yerine, cihazlara özel IP adresleri verir ve bu adresleri operatör ağının içinde sunulan NAT cihazları üzerinden tek veya sınırlı sayıdaki public IP adresi ile paylaştırırlar. Bu büyük ölçekli NAT uygulamasına Carrier-Grade NAT denir; bu uygulama sayesinde aynı public IP adresi yüzlerce veya binlerce kullanıcı tarafından paylaşılabilir hâle gelir. Bu yöntem IPv4 adres kıtlığını hafifletir ancak dışarıdan yapılan bağlantıların doğrudan bireysel cihaza yönlendirilmesini engeller ve IP adresinin fail tespitinde bireysel olarak kullanılmasını zorlaştırır çünkü bir IP adresi artık aynı anda birçok kullanıcıyla ilişkilendirilebilir.



Neticede IP adresinin her zaman faili doğrudan göstermediği, çeşitli teknik yöntemlerle gizlenebildiği veya yanıltılabildiği, tek başına kesin bir kimlik tespiti aracı olmadığı açıkça görülmektedir. Bilişim altyapısının işleyişi dikkate alındığında IP adresine dayalı tespitler, ancak IP'nin nasıl elde edildiği, hangi ağ koşullarında kullanıldığı ve hangi teknik ihtimallerin dışlandığı açıkça ortaya konulabildiği ölçüde anlamlıdır. Aksi hâlde IP adresi teknik olarak faili değil, yalnızca bir aktarımın görünümünü ifade eder. Bu teknik gerçeklik, IP adresine dayalı delil değerlendirmelerinin ne denli dikkatle ele alınması gerektiğini ve yapılabilecek potansiyel itirazları ortaya koymaktadır.

KAYNAKÇA:

1. https://www.hukukihaber.net/ceza-muhakemesinde-ip-adresi-log-kayitlari-ekran-ciktisi-ve-cgnat-his-verilerinin-ispat-degeri

2. https://www.legaltalks.com.tr/bilisim-sucluna-giden-yol-ip/#:~:text=Big%20Brother%20program%C4%B1%20bir%20a%C4%9F,ayr%C4%B1nt%C4%B1l%C4%B1%20bir%20log%20raporu%20alabilirsiniz

3. (https://www.a10networks.com/news/press-releases/turkcell-deploys-hyperscale-virtualized-carrier-grade-network-address-translation-from-a10-networks/?)

4. chttps://toptan.turktelekom.com.tr/media/yg5isbhi/pts-ek-protokol-010422.pdf?

DİJİTAL MİRAS

AV. SELİN AKGÜN

GİRİŞ

İnsanlık tarihi boyunca miras kavramı, maddi varlıklar üzerinden şekillenmiş; taşınır ve taşınmaz mallar, alacaklar ve borçlar, miras hukukunun ana eksenini oluşturmuştur. Ancak insanların günlük yaşamlarının büyük bir bölümünü sanal dünyada geçirmeye başlaması ve dijital varlıkların nitelik ve niceliklerinde yaşanan artışa bağlı olarak hemen hemen herkesin bir dijital varlığa sahip olması, hak sahiplerinin vefat etmelerinden sonra dijital varlıklar üzerindeki hakların kimler tarafından kullanılacağı ve dijital varlıkların akıbetinin ne olacağı meselelerini hukukun güncel tartışma konularından birisi haline getirmiştir. Bu gelişmeler doğrultusunda "dijital miras" kavramı, klasik miras hukukunun yerleşik sınırlarını zorlayan ve güncel hukuki tartışmaların merkezinde yer alan yeni bir problem alanı olarak karşımıza çıkmaktadır.

Dijital mal varlığı, kişilerin dijital ortamda sahip oldukları ya da kullandıkları hak, alacak ve borçların bütününü ifade eden bir kavramdır. Başka bir ifadeyle dijital mal varlığı, klasik miras hukukunun temel bir kavramı olan ve para ile ölçülebilen her türlü menkul ve gayrimenkul mal, hak, alacak ve borçların bütünü olarak tanımlanan mal varlığının bünyesinde dijital varlıkları barındıran halidir. Ancak burada dikkat edilmesi gereken nokta, maddi bir değeri bulunmasa dahi dijital ortamda mevcut olan her türlü veri ve değerin dijital mal varlığı niteliğinde olmasıdır. Klasik miras hukukunda olduğu gibi dijital varlıklar arasında da intikale elverişli olan ve intikale elverişli olmayan ayrımı yapılarak bir değerlendirme yapılması gerekmektedir.

Dijital mirasa gelirsek; teknolojinin her geçen gün gelişmesi ve bu gelişmeye bağlı olarak insanların ilk defa karşılaştığı dijital olguların ortaya çıkması nedeniyle dijital miras kavramına ilişkin öğretide üzerinde uzlaşılan, tek ve genelgeçer bir tanım bulunmadığını belirtmek gerekir. Bir tanımlama yapmak gerekirse bireyin yaşamı boyunca oluşturduğu, kullandığı veya sahip olduğu dijital hesaplar, veriler, içerikler ve dijital hakların ölüm sonrasındaki hukuki akıbetini ifade eder demek mümkündür. Dijital miras kavramı, tereke içerisinde yer alan dijital varlıkları ifade eden bir üst kavram olarak kullanılmaktadır. Sosyal medya hesaplarından e-posta arşivlerine, bulut depolama alanlarından kripto varlıklara kadar geniş bir yelpazeye yayılan bu dijital evren, hem özel hayatın gizliliği hem de mirasçıların hakları açısından ciddi tartışmaları beraberinde getirmektedir.

DİJİTAL MİRAS KAVRAMI VE KAPSAMI

Dijital miras kavramı, öğretide farklı şekillerde tanımlanmakla birlikte, genel kabul gören yaklaşım; miras bırakanın ölümünden sonra dijital ortamda varlığını sürdüren ve ekonomik ya da manevi değeri bulunan tüm dijital unsurların bu kapsamda değerlendirilmesi yönündedir. Dijital miras kavramına ilişkin önemli çalışmalardan birini kaleme alan Eşref Can Gürbüz'e göre dijital miras; "kişinin dijital dünyada oluşturduğu hukuki ve fiili varlığın ölümden sonra miras hukuku bağlamında değerlendirilmesini gerektiren unsurlar bütünü" olarak tanımlamakta ve bu alanın klasik miras hukukundan bağımsız düşünülemeyeceğini vurgulamaktadır.

Bu kapsamda dijital mirasın unsurları şu şekilde sınıflandırılabilir:

1-Dijital hesaplar: Sosyal medya profilleri, e-posta hesapları, çevrim içi üyelikler vb.

2-Dijital veriler: Fotoğraflar, videolar, yazışmalar, belgeler vb.

3-Dijital ekonomik değerler: Kripto paralar, NFT'ler, çevrim içi oyun varlıkları vb.

4-Dijital fikri ürünler: Blog yazıları, dijital sanat eserleri, çevrim içi içerikler vb.

Bu unsurların bir kısmı doğrudan ekonomik değere sahipken, bir kısmı mirasçılar açısından daha çok manevi değer taşımaktadır. Ancak her iki durumda da hukuki koruma ve tasarruf ihtiyacı açıktır.

TÜRK MEDENİ HUKUKU AÇISINDAN DİJİTAL MİRAS

Türk Medeni Kanunu'nda dijital mirasa ilişkin açık bir düzenleme bulunmamaktadır. Bununla birlikte, TMK'nın 599. Maddesinin 2. Fıkrası gereğince, gayrimenkul ve diğer mülkiyet hakları, sınırlı ayni haklar, taşınır ve taşınmazlara ilişkin zilyetlikler, borçlar ve yükümlülükler mirasçılara intikal eden kalemlerdir. Söz konusu madde metninden anlaşılacağı üzere, intikal edecek hak ve yükümlülükler *numerus clausus* (sınırlı sayıda) olarak sayılmamaktadır, bunun bir sonucu olarak, maddede bahsedilmeyen haklar da miras yoluyla intikal edebilecektir, *örneğin* fikri mülkiyet hakları mirasçılara devredilebilmektedir. Ne var ki dijital varlıkların niteliği, bu genel ilkenin uygulamasını her zaman kolay kılmamaktadır.

Özellikle kişisel nitelik taşıyan dijital hesaplar bakımından, "kişiye sıkı sıkıya bağlı haklar" kavramı gündeme gelmektedir. Sosyal medya hesapları ve özel yazışmalar, mirasçılara aynen devredilebilecek bir malvarlığı unsuru mudur, yoksa miras bırakanın şahsına bağlı haklar kapsamında mı değerlendirilmelidir?

Öğretide bu konuda tam bir görüş birliği bulunmamaktadır.

Gürbüz'e göre, dijital varlıkların tamamını tek tip değerlendirmek yerine, her bir dijital unsurun niteliğine göre ayrı ayrı hukuki değerlendirme yapılması gerekmektedir. Ekonomik değer taşıyan dijital varlıkların terekeye dahil edilmesi gerektiği açıkken, kişisel veri niteliği ağır basan dijital içeriklerde daha sınırlı bir mirasçı yetkisi öngörülmelidir.

KİŞİSEL VERİLER, ÖZEL HAYAT VE DİJİTAL MİRAS

Dijital miras tartışmalarının en hassas noktalarından biri, kişisel verilerin korunması ve özel hayatın gizliliğidir. 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin ölümle birlikte otomatik olarak korunma kapsamı dışına çıktığına dair açık bir hüküm içermemektedir. Bu durum, mirasçıların dijital verilere erişim talepleri ile miras bırakanın özel hayatının ve kişisel verilerinin korunması arasındaki dengeyi daha da hassas bir hale getirmektedir.

Özellikle e-posta yazışmaları, özel mesajlar ve kişisel fotoğraflar bakımından, mirasçıların sınırsız erişim hakkı olduğu kabul edilirse, bu durumun ölen kişinin iradesine ve mahremiyetine aykırı sonuçlar doğurabileceği hususu açıktır. Bu nedenle dijital miras meselesi, yalnızca miras hukuku açısından değil; aynı zamanda kişilik hakları ve veri koruma hukuku perspektifinden de ele alınmalıdır.

SOSYAL MEDYA PLATFORMLARI VE SÖZLEŞMESEL ENGELLER

Dijital mirasın uygulanmasında karşılaşılan bir diğer temel sorun, dijital platformların kullanıcı sözleşmeleridir. Birçok sosyal medya ve dijital hizmet sağlayıcısı, kullanıcı hesaplarının devredilemeyeceğine ilişkin hükümler içermektedir. Bu durum, mirasçıların hukuki talepleri ile platformların sözleşmesel düzenlemeleri arasında ciddi bir çatışma yaratmaktadır.

Uygulamada, bazı platformlar hesapların "anı sayfasına" dönüştürülmesine izin verirken, bazıları hesapların tamamen silinmesini tercih etmektedir. Ancak bu uygulamaların büyük çoğunluğu, Türk hukuku bakımından mirasçıların haklarını güvence altına alan bağlayıcı ve yeterli bir çözüm niteliği taşımamaktadır. Zira miras hukuku kamu düzeniyle yakından ilişkilidir ve sözleşme hükümleriyle bertaraf edilmesi her zaman mümkün değildir.

VASİYET, ÖLÜME BAĞLI TASARRUFLAR VE DİJİTAL MİRAS PLANLAMASI

Dijital mirasın en sağlıklı şekilde yönetilmesinin yolu, miras bırakanın sağlığında iradesini açıkça ortaya koymasından geçmektedir. Dijital varlıkların akıbetine ilişkin vasiyetname düzenlenmesi, bu alandaki belirsizlikleri büyük ölçüde azaltmaktadır. Miras bırakan, hangi dijital hesaplara kimlerin erişebileceğini, hangilerinin silinmesini istediğini açıkça belirleyebilir.

Bu noktada dijital miras planlaması, klasik malvarlığı planlamasının ayrılmaz bir parçası haline gelmiştir. Özellikle yüksek ekonomik değere sahip dijital varlıklar bakımından, bu planlamanın yapılmaması ciddi hak kayıplarına yol açabilmektedir.

DEĞERLENDİRME VE SONUÇ

Dijital miras, modern toplumun kaçınılmaz bir hukuki gerçeğidir. Mevcut mevzuat, bu yeni miras türünü düzenlemekte yetersiz kalmakta; uygulamada ciddi belirsizlikler yaşanmaktadır. Türk hukukunda dijital mirasa ilişkin açık ve kapsamlı bir yasal düzenleme yapılması, hem mirasçıların haklarının korunması hem de ölen kişinin iradesinin ve mahremiyetinin güvence altına alınması açısından zaruridir.

Bu süreçte, öğretinin ve yargı kararlarının yol gösterici rolü büyüktür. Hukukun dijitalleşme olgusuna uyum sağlaması, günümüz koşullarında artık bir tercih değil, hukuki bir zorunluluk olarak karşımıza çıkmaktadır.

KAYNAKÇA:

1. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

2. 4721 Sayılı Türk Medeni Kanunu

3. Gürbüz, Eşref Can, *Dijital Miras*, Adalet Yayınevi, Ankara, 2024.

4. https://dergipark.org.tr/tr/pub/inuhfd/article/466395 İnönü Üniversitesi Hukuk Fakültesi Dergisi,"Dijital Miras Kavramı ve Hukuki Niteliği",

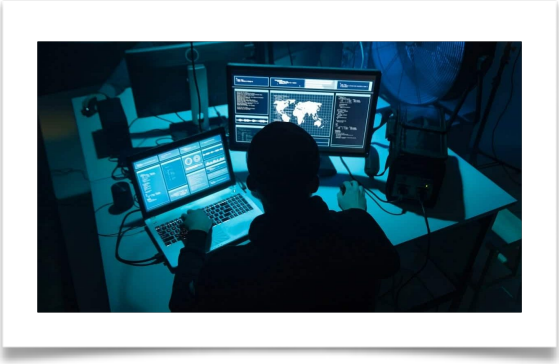
5. https://dergipark.org.tr/tr/pub/ahbvuhfd/article/871081Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, "Türk Hukuku Çerçevesinde Dijital Miras", DergiPark

SİBER SALDIRILARIN GÖLGESİNDE 2025

AV. AHMET KALKAN

Uzun bir süre siber saldırılar, hukuk dünyasında tali bir mesele gibi ele alındı. Teknik uzmanların, bilişim birimlerinin ya da büyük şirketlerin iç sorunu olarak görüldü. Oysa 2025 yılı, bu yaklaşımın artık sürdürülemez olduğunu açık biçimde ortaya koydu. Bugün siber saldırılar; bireyin mahremiyetinden kamu hizmetlerinin sürekliliğine, ekonomik istikrardan ulusal güvenliğe kadar uzanan geniş bir alanı doğrudan etkileyen gerçek ve somut tehditler hâline gelmiş durumda.

Artık saldırılar yalnızca "bir sistemin çökmesi"nden ibaret değildir. Hastanelerin hizmet veremediği, belediyelerin işleyemez hâle geldiği, üretim tesislerinin günlerce durduğu olaylardan söz ediyoruz. Daha da önemlisi, bu olayların büyük bir kısmı tesadüfi ya da münferit değil; planlı, organize ve çoğu zaman sınır aşan yapılar tarafından gerçekleştirilmektedir.



2025 yılında ses getiren büyük siber saldırılara bakıldığında ortak bir tablo ortaya çıkmaktadır: Kritik altyapılar hedef alınmaktadır. Sağlık, enerji, ulaşım ve kamu hizmetleri gibi alanlar, siber suç grupları için en etkili hedefler hâline gelmiştir. Bu alanlara yönelik saldırılar yalnızca ekonomik zarar doğurmakla kalmamakta, aynı zamanda kamu düzenini ve toplumsal güvenliği de doğrudan etkilemektedir.

Bu noktada siber saldırılar ile klasik sabotaj eylemleri arasındaki fark giderek silikleşmektedir. Fiziksel saldırılar ile dijital saldırıların sonuçları arasındaki ayrım büyük ölçüde ortadan kalkmıştır. Buna karşın hukuki düzenlemelerin bu dönüşüme aynı hızla ayak uydurduğunu söylemek güçtür.

Özellikle ransomware saldırılarının geldiği nokta, hukuki boşlukları daha görünür kılmıştır. Fidye yazılımları artık yalnızca veri şifreleyen araçlar değil; kurumları müzakereye zorlayan, kamuoyunu etkileyen ve çoğu zaman hukuki belirsizliklerden beslenen sistemlerdir.

Bir siber saldırı sonucunda milyonlarca kişinin kişisel verisi sızdığında sorumluluk yalnızca saldırıyı gerçekleştiren faillerde aranmamalıdır. Gerekli teknik ve idari tedbirleri almayan veri sorumlularının da hukuki sorumluluğu bulunmaktadır. Siber güvenlik artık bir tercih değil, açık bir yükümlülüktür.

Yapay zekâ destekli saldırı tekniklerinin yaygınlaşması ise sorunu daha da karmaşık hâle getirmektedir. Otonom sistemler tarafından yönlendirilen saldırılar, klasik ceza hukuku kavramlarının yeniden değerlendirilmesini zorunlu kılmaktadır. Kast, kusur ve ihmal gibi kavramlar insan iradesi üzerinden şekillenmişken, algoritmik karar mekanizmalarının etkisi bu alanı belirsizleştirmektedir.

2025 yılı, siber güvenliğin teknik bir konu olmanın ötesinde hukuki ve toplumsal bir mesele olduğunu net biçimde ortaya koymuştur. Kurumların ve kamu otoritelerinin "henüz başımıza gelmedi" anlayışı artık kabul edilebilir değildir.

Önleyici hukuk yaklaşımı bu alanda kaçınılmazdır.

Sonuç olarak, dijital çağın sessiz saldırıları karşısında hukuk suskun kalamaz. Siber saldırılar artık geleceğin değil, bugünün meselesidir. Hukukun bu alandaki refleksi geciktikçe bedelini toplum ödemektedir.