



Bu proje Avrupa Birlięi tarafından finanse edilmektedir.



National Programme for Turkey 2014 – 2020
Instrument for Pre-Accession Assistance II

Hâkim ve Savcı Adaylarının Staj Verimlilięinin ve Etkinlięinin Arttırılması Projesi

Sözleşme No.: TR2015/RL/03/A3.5-01
Referans No.: EuropeAid/162288/ID/ACT/TR

Dijital Delillerin Deęerlendirilmesi

Hazırlayan Uzmanlar:

Rafael FERNÁNDEZ DE PAIZ, Savcı

Jesús Ángel SUÁREZ RAMOS, Kıdemli Hâkim

Bu proje Türkiye Cumhuriyeti ve İspanya Krallığı arasında yürütölen bir eşleştirme ortaklığıdır.



Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

İÇİNDEKİLER

Dijital Delillerin Değerlendirilmesi	2
1.- Giriş	2
2.- Elektronik delilin özellikleri	3
3.- Elektronik delillerin elde edilmesi, işlenmesi ve muhafaza edilmesinden etkilenen temel haklar.....	4
4.- Hukuken derecelendirilmesi gereken şartlar	8
5.- Elektronik delillerin hukuken derecelendirilmesine farklı katkılar ve buna ilişkin uygulama9	
5.1 Özel belgeler	9
5.2 Resmi belgeler.....	10
5.3 Teknoloji uzmanı raporu	11
5.4 İyi uygulamalar	12
5.5 Delil zinciri	13
6.- Avrupa Konseyi Bakanlar Komitesi'nin Adli ve İdari Yargılamalarda Elektronik Delillere Dair Kılavuz İlkeleri.....	14
6.1 Tanımlar	16
6.2 Temel prensipler	16
6.3 Kılavuz ilkeler	17
• Uzaktan ifade alma [Kılavuz ilke 1-5]	17
Elektronik delillerin kullanımı [Kılavuz ilkeler 6-9].....	18
• Delillerin toplanması, elde edilmesi ve iletimi [Kılavuz ilkeler 10-16].	20
• İlgililik [Kılavuz ilkeler 17 ve 18]	24
7.- Avrupa Soruşturma Emri aracılığıyla diğer ülkelerden nasıl elektronik delil talep edilir? (Karşılıklı Adli Yardımlaşma-Karşılıklı Adli Yardımlaşma Talebi)	25
GERÇEK DAVALAR VE TARTIŞMAYA YÖNELİK FİKİRLER.....	26
2.1 DAVA A (Nagla)	26
2.2 DAVA B (Elektronik delil ve zehirli ağacın meyvesi de zehirlidir teorisi).....	29
EK ÇALIŞMA MATERYALLERİ VE KAYNAKLARI	32
EĞİTİM PLANI	33
DEĞERLENDİRME FORMU.....	34



Dijital Delillerin Değerlendirilmesi

1.- Giriş

Vatandaşlar ve işletmeler arasındaki günlük ilişkilerde dijital teknolojilerin giderek artan kullanımı nedeniyle, mahkemelere ve adli işlemlere dijital delillerin getirilmesi ve değerlendirilmesi için yeni kuralların benimsenmesi bir gerekliliktir.

Dünya çapında kullanılan platformların ve teknolojinin, bölgesel sınırlar ve yasal sistemlerden bağımsız olarak esas olarak aynı olduğu tartışılmaz gerçeği, bu kaynakların yönetimi ve hakların adli korumasının iyileştirilmesi için pratik bir çerçeve oluşturmayı çok önemli kılmaktadır. Bilgi standart bir şekilde işlendiğinden, farklı ülkeler arasında kullanımda mevzuatın ve uygulamanın yakınlaştırılması çok uygun bir hedeftir.

Teknoloji aynı zamanda suçlular tarafından çok farklı suçlarda (cinsel sömürü, çocuk istismarı, dolandırıcılık, kara para aklama vb.) kullanılan güçlü bir araçtır

İnsan haklarının korunması, Avrupa Konseyi'nin amacıdır. Türkiye, 47 farklı üye devletten oluşan Avrupa Konseyi'ne 13 Nisan 1950 tarihinden beri üyedir. Konseyin dijital delillere ilişkin rolünün altı çizilmelidir:

- Adli yargıda ve idari yargıda: Üye devletler arasında yasal kuralların standart hale getirilmesi için kriterler önerilmesi ihtiyacını fark eden Bakanlar Komitesi, 30 Ocak 2019 tarihinde (Bakan Yardımcılarının 1335. toplantısı), Avrupa Konseyi Bakanlar Komitesi'nin adli ve idari yargılamaalarda elektronik delillere ilişkin kılavuz ilkeleri kabul etmiştir. Bu ilkelerin “pratik bir araç olarak tasarlanan ve bu alandaki ilk uluslararası belge” olduğu düşünülmektedir.

- Ceza hukukunda, Avrupa Konseyi üye devletleri, 23.11.2001 tarihli Siber Suçlar Sözleşmesi'ni (Budapeşte Sözleşmesi) kabul etmiştir (Türkiye'de 01.01.2015 tarihinden bu yana yürürlüktedir). Sözleşme, internet ve diğer bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası sözleşmedir ve özellikle telif hakları ihlalleri, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlalleriyle ilgilidir. Ayrıca bilgisayar ağlarının aranması ve bilgisayar ağlarına müdahale gibi bir dizi yetki ve usul içermektedir.

Sözleşmenin amacı, giriş kısmında da belirtildiği üzere, özellikle uygun mevzuatı kabul ederek ve uluslararası iş birliğini güçlendirerek toplumun siber suçlara karşı korunmasını amaçlayan ortak bir ceza politikası izlenmesidir. Üye devletler, “Bilgisayar ağlarının ve elektronik verilerin, suç işlemek için kullanılabilme ihtimali ve bu tip suçlara dair kanıtların, saklanılabilirliği ve bu ağlar tarafından iletilirliği ile ilgili endişelenmiştir [...] Siber suçla mücadele ve bilgi teknolojilerinin kullanımı ve gelişimindeki meşru menfaatlerin korunması gerekliliği ile ilgili Devletler ve özel sektör arasındaki iş birliğinin gerekliliğini tanımıştır”.



Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Sözleşmenin 4. Başlığı (saklanan bilgisayar verilerinin araştırılması ve alıkoyulması) ve 5. Başlığı (bilgisayar verilerinin gerçek zamanlı toplanması), teknoloji kullanımı ve elektronik verilerin toplanmasıyla ilgili birçok konuyu içermektedir.

2.- Elektronik delilin özellikleri

Geleneksel delillerle kıyaslandığında, elektronik delillerin özellikleri şu şekildedir:

- **Soyut:** Elektronik deliller elektronik formattadır, çoğaltılabilir, kopyalanabilir, delillerin asıllarının nüshalarından ayırt edilmesi olasılığı düşüktür.
- **Geçici:** Elektronik deliller, taklit edilebilir, değişkendir, nihayetinde yönlendirilebilir, yani kolayca değiştirilebilir.¹
- **Hassas:** Elektronik delillerin hem gelişigüzel bir şekilde hem de kasten imha edilmesi kolaydır. Aslında elektronik bir dosya basit bir talimatla silinebilir. Yukarıdakiler doğru olsa da bilgisayarların sabit disklerini silmek görüldüğü kadar kolay değildir. Bu nedenle, kişisel bir bilgisayardaki bir dosya silindiğinde, bu dosya aslında sabit diskten silinmez fakat diskin o kısmına girilmesin diye silinmiş olarak görünür.
- **Tek taraflı:** Elektronik işlemler her zaman hazır bulunmayan kişiler arasında gerçekleşir. Bu işlemlerin olması için dahil olan tarafların, genellikle taraflardan birinin sahip olduğu ve kontrol ettiği bir bilgisayar kaynağına yaklaşması gerekmektedir. Buna net bir örnek, bir tür hizmet sunulan internet sayfalarına erişimdir. Bunu yapan kişinin ayrıca bu internet sitesini oluşturan bilgisayar kaynakları üzerinde teknik kontrolü vardır ve bu nedenle bu internet sitesinde neler olduğuyla ilgili elektronik delil oluşturabilecek tek kişidir. Bu kişi aynı zamanda internet sitesinde olanlarla ilgili bilgisayar kayıtlarını değiştirme veya silme olasılığı olan kişidir.
- **Aracılık:** Deliller, yargılamada sunulduktan sonra hemen gösterilirken, elektronik delillerin görüntülenebilmesi için ilgili donanım ve yazılımın olması gerekmektedir. Bu nedenle, yargılamada yazılı bir dilekçe sunulursa, bu dilekçeyi okuyan herkes, eğer dilekçede kullanılan dili biliyorsa, dilekçenin içeriğini anlayacaktır. Fakat gönderilen e-postayı içeren bir dosyanın yer aldığı bir flaş bellek verilirse, bir bilgisayar ve uygun bir e-posta yönetim yazılımının (gmail, outlook...) olması gerekecektir. Kısacası, yazılı deliller hemen görüntülenirken, elektronik delillerin bir donanım veya yazılımdan geldiği ve bu nedenle delillerin uygulanmasının aksaklıklara neden olabileceği sonucuna varılabilir.
- **Müdahaleci:** Bazen elektronik delillerin toplanması, hepsi olmasa da özel hayatın gizliliği hakkı, haberleşmelerin gizliliği hakkı, dernek kurma özgürlüğü veya kişisel verilerin korunması gibi temel hak ve özgürlükleri etkileyebilir. Aslında hazır bulunmayan kişiler arasındaki elektronik ilişkiler, iletişimi sürdüren taraflar arasında iletişim süreçleri

1 Benzer şekilde, Yüksek Mahkeme'nin 2. Dairesi'nin 19 Mayıs tarihli 300/2015 sayılı kararında şu husus yer almaktadır: Görüş alışverişinin neden olduğu dijital dosyaların manipüle edilme olasılığı, nesnelerin gerçekliğinin bir parçasıdır.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

gerektirmektedir. Bir iletişim sürecinden delil elde edilmesi, haberleşmelerin gizliliği hakkına ve/veya bu iletişim sürecine dahil olan kişilerin özel hayatının gizliliğine müdahale edilmesine yol açabilir. Bu nedenle, elektronik işlemlere ilişkin delil elde edilmesi işlemleri, temel hakların ihlal edilmemesine neden olmamalıdır. Kısaca, delilin elektronik olması, kaynağa erişimde hukuka uygunluk şüphesi uyandırır ve açıklaması güç olan haksızlıklara karşı itirazlar için fırsat sunar.

3.- Elektronik delillerin elde edilmesi, işlenmesi ve muhafaza edilmesinden etkilenen temel haklar

Elektronik deliller, temel hakların ihlal edilmesini içeriyorsa elde edilemez veya işlenemez. Çünkü bu durum, delili geçersiz kılacaktır. Bu nedenle, delillere erişim, usul kuralları ve güvenceler gözetilerek yapılmalıdır:

- Haberleşmelerin gizliliği

Haberleşmelerin gizliliği kavramı, yalnızca haberleşmenin içeriğini değil aynı zamanda muhatapların “doğru bir şekilde anlaşılabilmesi” için muhatapların kimliğini de kapsamaktadır. Haberleşme kavramının nesnel kapsamı, tartışmasız bir şekilde, haberleşmenin dışındaki üçüncü taraflarca (kamu veya özel: bu hakkın herkes bakımından geçerli bir etkililiği vardır) girilememesinin sağlanmasını amaçlamaktadır. Bu nedenle, polisin, muhataplardan biri erişim yetkisi verdiği için polisin iki kişi arasındaki konuşmaların içeriğine müdahale edebileceği doktrinsel olarak tartışılmaktadır. Bu konuşma, muhataplardan biri devletin müdahalesini kabul etmiş olsa bile, kanunların uygulanması amacıyla devlet yetkilileri tarafından gözlemlenir veya dinlenirse anayasal olarak itiraz edilebilir olacaktır (AİHM Kararları. 24.2.90 tarihli *Kostowski ve Fransa* davası, 5.11.2002 tarihli *Allan ve Birleşik Krallık* davası of (AİHM 2002, 64), 8.4.2003 tarihli *M.M. ve Hollanda* davası (JUR 2003, 244791)). Haberleşmelerin gizliliği, suçların önlenmesi veya ortaya çıkarılması genel ihtiyacının karşılanması veya soruşturmacıların nesnel olarak dayanaksız şüphelerini gidermek için açıklanamaz. Yoksa anayasal güvence zayıflatılır.

Temel hak, üstü kapalı olarak haberleşme özgürlüğünü ve haberleşmeye müdahale edilmesini veya yasa dışı olarak haberleşmenin bilinmesini yasaklayarak açıkça haberleşmenin gizliliğini kabul etmektedir. Fakat muhataplar açısından gizlilik yükümlülüğü bulunmamaktadır ancak her halükarda, iletilen mesajın içeriğine bağlı olarak olası bir “çekince koyma yükümlülüğü” vardır. Bu nedenle, haberleşmelerin gizliliği temel hakkı ile özel hayatın gizliliği temel hakkı arasında farklılıklar vardır. Çünkü bir telefon konuşması, e-posta, WhatsApp konuşması bağlamında, telefonu hoparlör moduna alan, e-postayı, WhatsApp mesajını veya SMS'i





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

başkalarına gösteren kişi, eyleme hâle getirmeksizin haberleşmenin gizliliğini ihlal etmemektedir. Fakat mesajı ileterek ve mesajı veren kişinin “yakın” çevresine giren üçüncü tarafları bilgilendirerek özel hayatın gizliliğini ihlal edebilir.

Bu bağlamda, *zehirli ağacın meyvesi de zehirlidir* doktrininden bahsedilmesi dikkate değer bir noktadır. Delil, elde edildiği kaynak hukuka aykırı olduğu için ilke olarak mahkemede kabul edilmeyecek olsa bile (“zehirli ağaç doktrininin meyvesi: zehirli ağacın meyvesi zehirlidir”) kaçınılmaz keşif doktrini uygulanırsa kabul edilebilir hale gelir (koşullar nedeniyle, zehirli ağaç doktrinine göre delili kabul edilemez kılan yasa dışı faaliyet olmasa bile herhangi bir şekilde delilin elde edilebilmesi durumu).

İspanya Devlet Başsavcılık Ofisi’nin telekomünikasyon alanında kişisel verilerin otomatik olarak işlenmesi hakkında 22 Ocak tarihli 1/1999 sayılı Müzakeresinde (RCL 2000, 878), “anayasal dokunulmazlığın sadece bir mesajın içeriğine veya haberleşmenin önemli koşullarına gerçek zamanlı olarak müdahale edilmesini veya bunların toplanmasını değil aynı zamanda bunlar hakkında yasa dışı olarak bilgi edinilmesini de engellediği” belirtilmiştir. Bu nedenle, e-postalara müdahale edilmesine ilişkin güvenceler, normal posta müdahalesine ilişkin güvenceler değildir. Aksine, hedeflenecek e-posta hesaplarına ilişkin mahkeme kararıyla kimlik tespiti dahil olmak üzere telefon dinlemesine ilişkin güvencelerle aynıdır. Hakkında soruşturma yürütülen kişi tarafından kullanılan telefon hattının belirlenmesi tek başına iyi bir uygulama değildir çünkü söz konusu kişi, e-posta hesabına diğer hatlar aracılığıyla erişebilir.

Bu nedenle, anayasal kuralların ihlaliyle elde edilen deliller faydalı değildir. Örneğin, iletişimin gizliliği hakkı, sohbetlerde yer alan bilgiler mahkemede kullanılamadığında ihlal edilmektedir.

https://www.fiscal.es/memorias/estudio2016/CIR/CIR_01_1999.html

Mahremiyet ve öz imaj

Güvence altına alınan kişisel mahremiyet ve öz imaj hakları, özel hayat kapsamına giren kişisel varlıkların bir parçasıdır. Bu haklar, mahremiyetle ilgili verilerin ve koşulların toplanması ve dağıtımına ilişkin araçlar ve usulün geliştirilmesine karşı gerekli korumanın altı çizilerek değişik müdahalelerden muaf tutulan bir alan olarak kişisel ve aile mahremiyetiyle korunmaktadır. Bu bağlamda, mahremiyet alanına giren unsurların, veri sahibi kişinin mahremiyetinin yansıtılabileceği unsurlar olduğu ileri sürülebilir. Bu nedenle, mahremiyete müdahalenin geçerliliğini sağlamak amacıyla anayasal meşruiyeti gözetken bir adli yetki gerekmektedir. Bu hakkın kısıtlanmasına ilişkin karar, tedbirin meşruiyeti, orantınlılığı ve gerekliliğine ilişkin bir kararla yalnızca hakimlere ve savcılara bırakılmalıdır. Bu karar, ceza davası kapsamında alınan gerekçeli kararın içinde olmalıdır ve bu nedenle bazı hususları ele almak zorundadır:





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Orantılılık: Ağır bir suçun soruşturulması kapsamında olmalıdır. Hapis cezası kararının yalnızca hukuki öngörüsü ele alınmamalı aynı zaman soruşturulacak suçun toplumsal önemi de değerlendirilmelidir.

Özellik: Müdahale, genel olarak bir kişinin davranışının incelenmesini amaçlayan yasal gözlemler olmadan belli bir suçun soruşturulmasıyla ilgili olmak zorundadır.

Bireysellik ve uygunluk: Özellikleri ve koşulları göz önünde bulundurulduğunda soruşturulan temel haklar için daha az yüklenmiş olan ve soruşturma için eşit derecede faydalı olan diğer tedbirler, soruşturma için mevcut olmadığında makul bir bakış açısıyla tedbirin bireyselliği ve uygunluğuna karar verilmelidir.

Kişisel verilerin korunması

Kişisel verilerin korunması hakkı, AVRUPA BİRLİĞİ TEMEL HAKLAR ŞARTININ (2000/C 364/01) 8. maddesinde temel bir bireysel hak olarak belirtilmektedir:

"Kişisel verilerin korunması. 1. Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. 2. Bu veriler, adil bir şekilde, belirli amaçların ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. 3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir".

http://www.europarl.europa.eu/charter/pdf/text_es.pdf 2 Nisan 2018 tarihinde alınmıştır

Avrupa Birliği Sivil Servis Mahkemesi'nin 5 Temmuz 2011 tarihli kararının (ROJ: STFPUE 6/2011 - ECLI:EU:F:2011:101) 1. kısmında belirtildiği üzere, bu hükmün yorumlanmasıyla, İçtihatla, bu hakkın özelliklerine ilişkin olarak şu belirtilmektedir:

"Mahkemenin içtihadına göre, AİHS'nin 8. maddesinde belirtilen ve Üye Devletlerin ortak anayasal geleneklerinden gelen özel hayata saygı hakkı, AB yasal düzeniyle korunan temel haklardan birini oluşturmaktadır. Bu hak, özellikle, sağlık durumunun gizli tutulması hakkını içermektedir (bkz, özellikle, Adalet Divanı'nın 5 Ekim 1994 tarihli kararı, X ve Komisyon davası, C-404/92 P , paragraf 17, ayrıca bkz. AİHM, 25 Şubat 1997 tarihli Z ve Finlandiya kararı, Recueil des arr'ets et décisions 1997-I, paragraf 71 ve 30562/04 ve 30566/04S başvuru numaralı 4 Aralık 2008 tarihli Marper ve Birleşik Krallık davası, paragraf 66). 112. Bir kişinin sağlık durumuna ilişkin bir kurumun kendisi tarafından toplanan kişisel verilerin, başka bir kurum dahil olmak üzere, üçüncü bir tarafla paylaşılması, iletilen veriler daha sonra ne şekilde kullanılırsa kullanılsın, ilgili kişinin özel hayatına müdahale anlamına gelir (bkz, kıyas yoluyla, Adalet Divanı'nın 20 Mayıs 2003 tarihli sterreichischer Rundfunk and Others davası, C-465/00, C-138/01 ve C-139/01, paragraf 73-75). 113. Ancak kamu yararına hedefleri karşılamaları ve ulaşılmak istenen hedef açısından güvence altına alınan hakkın





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

özünü aşırı ve kabul edilemez bir şekilde etkilememesi koşuluyla temel hakların kısıtlamalara tabi olabileceğine karar verilmiştir (5 Ekim 1994 tarihli karar, X ve Komisyon davası, paragraf 18). Bu bağlamda, AİHS Madde 8(2)'ye atıfta bulunulmak zorundadır. Bu hüküm kapsamında, kamu kurumlarının özel hayata müdahalesi ancak şu durumlarda gerekçelendirilebilir: (i) "yasa ile öngörülmüş olması", (ii) belirli amaçlar için olması ve (iii) bu amaca veya amaçlara ulaşmak için "gerekli" olması."

Kişisel verilerin korunmasına ilişkin yakın zamanda yeni bir tüzük yürürlüğe girmiştir: *Kişisel verilerin işlenmesi karşısında gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin 2016/679/AB sayılı Tüzük*. Ancak bu kurallar doğrudan ceza davalarına uygulanmamaktadır. Ceza davalarında, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair 2016/680 sayılı Direktif² uygulanmaktadır.

- Tavsiyeler:

Adli kararlarda kişisel verilerin açıklanması halinde, (c) özel bir koruma gerektiren mahremiyet hakkı ve kişilerin haklarının tam olarak gözetilmesini ve uygun olduğu hallerde mağdurların veya zarar gören kişilerin anonimliğini güvence altına almak amacıyla kararda yer alan kişisel verilerde kişilerin gerçek isimleri silinmelidir.

- Denetim makamı

Direktifte, Direktifte yer alan kurallara mahkemeler ve diğer yargı makamları (örneğin, savcılıklar) tarafından uyulmasının, Şartın 8.3 maddesi uyarınca (Gerekçe 80'nin son fıkrası), bağımsız bir denetime tabi olmak zorunda olduğu belirtilmektedir.

https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Ancak Direktifte aynı zamanda denetim kurumlarının yetkisinin, hakimlerin görevlerini bağımsız bir şekilde yerine getirmelerini sağlamak amacıyla, mahkemelerin yargısal faaliyetlerini yerine getirdiği hallerde (Gerekçe 80), kişisel verilerin işlenmesini kapsamaması gerektiği belirtilmektedir.

Bu nedenle, Direktifin 45. maddesinin ilk fıkrasında, "Üye Devletler, denetleyici makamların, mahkemelerin adli yetkilerinde hareket ederken yapmış oldukları veri işleme faaliyetlerinin denetimi hususunda yetkili olmamasını sağlayacaktır" ifadesi yer almaktadır.

² Genel Veri Koruma Tüzüğü Madde 2.2(d) GDPR –EDL 2016/48900- Tüzük, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesine uygulanmaz."





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Yürürlükte olan İspanya mevzuatı uyarınca, kişisel verilerin korunmasına ilişkin mevzuatın hukuki amaçlarla ve bu mahiyetteki dosyalar için yürütülen veri işleme faaliyetleriyle ilgili İspanya Kişisel Verilerin Korunması Kurumu'na verdiği yetkiler, Hakimler Genel Kurulu tarafından yürütülür.

4.- Hukuken derecelendirilmesi gereken şartlar

Bu tür delillerin sanal mahiyetleri nedeniyle, varlığını kanıtlayan veri üstü verileri içeren bilgisayar dosyalarını ele geçirerek bunun belgelenmesi gerekmektedir. Ancak elektronik delilin yargı makamı tarafından kabul edilmesi için bunun bazı şartları karşılaması gerekmektedir:

- **Kanuna uygunluk:** Elektronik delillerin elde edilmesinin ilgili kişinin mahremiyet hakkını ihlal edemeyeceği ve hiçbir koşulda iletişimin gizliliğinin ihlal edilemeyeceği anlamına gelmektedir. Bu alanda, kararın orantılılığı, uygunluğu, gerekliliği ve gerekçesine ilişkin Anayasa Mahkemesi tarafından belirtilen doktrine de uyulması gerekmektedir ve kurumun çalışanlar tarafından kabul edilen bir Teknolojik Araçların Kullanımına ilişkin Politikası olmalıdır.
- **Bütünlük:** Delilin bütünlüğü sağlanmalıdır ve bunun için bilgisayarın içeriğinin kopyalanması ve herhangi bir çoğaltmayı belgeleyen HASH değerinin garanti edilmesi uygundur (HASH veriler bilgisayar biliminde yaygın bir uygulamadır ve birkaç farklı amaç için kullanılır. Örnekler arasında kriptografi, sıkıştırma, sağlama toplamı oluşturma ve veri indekslemeyi yer alır.).
- **Gerçeklik:** Hakkında soruşturma yürütülen veri örneklerinin, gerçek verilerle aynı olmasının sağlanması. Bu da Delil Zinciri korunarak sağlanmaktadır. Delil Zinciri, verilere erişilmesi, verilerin elde edilmesi, aktarılması ve saklanması sürecini belgeleyerek delilin değiştirilmemesini güvence altına almaktadır.
- **Netlik:** Bilgisayar teknisyeni olmayan ve sürece katılan taraflarca anlaşılması gerektiği anlamına gelmektedir.



5.- Elektronik delillerin hukuken derecelendirilmesine farklı katkılar ve buna ilişkin uygulama

Genel olarak, elektronik delil elde edilmesine ilişkin farklı yöntemler analiz edilmeden önce, böyle bir denetime ilişkin önceden bilgi vermeden çalışanın e-postasına erişim sağlanması gibi, herhangi bir tarafın temel haklarını ihlal ederek elde edilen delillerin, bu delil temelinde verilebilecek disiplin cezasının olası hükümsüzlüğüne halel getirmeksizin, mahkemede kabul edilmeyeceğinin belirtilmesi gerekmektedir.

5.1 Özel belgeler

- E-posta

Elektronik delil birçok şekilde uygulanabilmektedir. Bunlardan biri, örneğin, tasdik eden bir yetkili veya noterin müdahalesi olmadan bir e-postanın basılması ya da bir WhatsApp mesajının “taranması” gibi belli bir bilgisayar aracının doğrudan çıktısının alınmasıyla elde edilen özel bir belgenin sağlanmasıdır. Bu durumda, delil, gerçekliğı hakkında ciddi şüpheler uyandırarak ve sonuç olarak hâkimi geri kalan delillerle bağlantılı olarak bu delili değerlendirmeye zorlayarak kanıt değerini düşürerek, geri kalan delillerle birlikte bütünüyle değerlendirilecektir. Bu durum hatta delilin kendi başına bir belge olarak değerlendirilmesinin reddedilmesine bile yol açabilir.

- Ekran görüntüsü

Yüksek Mahkeme tarafından yürütölen *Tuenti* davasından özellikle bahsedilmelidir (İspanya Yüksek Mahkemesi, Ceza Dairesi, 19-5-15, Rec. 2387/2014). Bu önemli kararda, bir cinsel taciz davasında *Tuenti* sosyal ağından alınan ekran görüntülerinin geçerliliğı ve gerçekliğı yargılanmıştır. Yüksek Mahkeme, bu anlık mesajlaşma davalarındaki delillerin değerlendirilmesinin manipölasyon olasılığı ile “tüm dikkatle ele alınması gerektiğı” sonucuna varırken, bu durumda, diğör dolaylı delillerin değerlendirilmesi gerektiğı sonucuna varmıştır. Örneğın, mağdurun kendisi, ekran görüntülerini kolluk görevlilerinin huzurunda da alacak olan bir bilirkişisi raporu talep etmek için Soruşturma Hakimine Tuenti şifresini vermiştir veya mesajların diğör muhatabı duruşmaya tanık olarak katılmıştır.



Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

- Taraflar arasındaki sohbet veya cep telefonu mesajı

Hakim ve savcıların, bir sohbet veya anlık mesajlaşmayı bir belge olarak değerlendirmesi ve kabul etmesi için (kanıt değeri dışında) bunların aşağıdakilerden herhangi bir durumda olup olmadığını değerlendirmesi gerekmektedir:

- a) sohbetin muhataplarından birinin sohbete karşı çıkmaması,
- b) bu sohbet ve sohbetin içeriğinin açık bir şekilde kabul edilmesi,
- c) sohbetin gerçekliğinin, diğer ilgili tarafla kontrol edilerek doğrulanması,
- d) öncekilerden farklı bir varsayım için, görüşmenin gerçekliğini ve gönderilmesini doğrulayan bir bilirkişi incelemesi yapılması.

Bu nedenle, kanıtlama yükümlülüğü konuşmayı veya yayını yazılı delil olarak sunan kişiye aittir, burada yazılı delil sunumu artık yeterli veya açık olmayacaktır. Bu konuda bir bilgisayar uzmanı talep etme imkanı sağlayacaktır.

- Özel belgelere itiraz edilmesi

Savcılık özel belgenin gerçekliğine itiraz ederse, bu belgeye ilişkin bilirkişi görüşü sunmak zorundadır. Uygulamada, belgenin, belgeyi sunmayan tarafça tanınmadığının belirtilmesi yaygındır. Çünkü açıkça tanıma, süreçte söz konusu belgenin hem içerik hem de tarih ve kimlikler bakımından tam ispat değerine sahip olduğu ve taraflar tarafından kabul edildiği anlamına gelmektedir. Belgeye açıkça itiraz edilmemişse, adli değerlendirme, aksi yönde bir kanıt olmadıkça (*iuris tantum*) genellikle gerçekliğini varsayma eğilimindedir.

5.2 Resmi belgeler

Özel belgelerin aksine, resmi belgeler, sahtecilik olduğundan emin olmadıkça itiraza tabi değildir. Bu durumda, orijinal belgeyle çapraz kontrol edilmeleri veya belgeye müdahale eden görevli tarafından onaylanmaları istenecektir.

- Özel belgelerin içeriğinin resmi belgelere dahil edilmesi

Yukarıdaki örneklerin ardından, bir e-posta veya WhatsApp mesajını (sosyal medya belgeleri, web siteleri vb.) resmi bir belgeye dahil etmeyi seçerseniz, bu tür girdiler aşağıdakiler tarafından yapılabilir:

- (a) Kaydedildikleri cihaza erişip yazdırdıktan sonra mesajların varlığına dair kamu inancının sağlanacağı noterlik belgesi.

Hâkim ve savcı, tutanakların, mesajların gönderildiği veya alındığı e-posta adresini veya telefon numarasını, mesaj tarihlerini ve ayrıca katılımcıların kimliklerini içermesini sağlar.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

b) Resmi bir belgenin aynı kanıt değeri, ilgili tarafların talebi üzerine mahkemenin kendisinde uygulanacaktır (kamunun yargıya inancı). Bu durumda, belirli bir WhatsApp mesajının içeriğini, bu tür mesajlarda görünen kimlikleri ve kullanılan mobil cihazla ilgili tutanakları yayımlayan mahkeme katibi olacaktır. Bu tutanağa ayrıca orijinallik ve manipülasyon yapmama garantisinin bir artısı olarak bir bilgisayar uzmanının raporu eklenebilir.

5.3 Teknoloji uzmanı raporu

Hâkimler ve savcılar teknoloji uzmanı raporlarından neden haberdar olmalı ve bunları ne zaman talep etmelidir?

Çoğu elektronik delile, mahkemede sunulacak elektronik içerikten elde edilebilecek dijital delillerin "korunmasını" amaçlayan prosedürlerin geliştirilmesini içeren ve bir bilgisayar uzmanı tarafından hazırlanan bir rapor eşlik edecektir. Bu koruma, bu tür bilgilerin alfanümerik bir kodu (karma kod) ile sonuçlanan depolanan dijital bilgilerin "doğru" adli tıp kopyalarının yapılmasıyla elde edilir. Soruşturmanın sonuçları, bilirkişi görüşü olarak sunulacak ve daha sonra taraflarla yüzleşmek için mahkemede onaylanacak bir teknoloji uzmanı raporuna aktarılacaktır.

Bir bilgisayar uzmanı raporu aracılığıyla elektronik delil sağlamanın amacı, adli süreçte dijital delil olarak sunulan dijital bilgilerin orijinalliğini, gerçekliğini ve bütünlüğünü sağlamaktır. Bu nedenle, bu seçenek, bir bilgisayarın sabit diski gibi analiz edilecek büyük miktarda veri ve bilginin olduğu veya elektronik delilin birincil, hatta mevcut tek delil olduğu ve mobil uygulama mesajları gibi manipülasyon şüpheleri olan durumlarda yararlı olacaktır.

Bu tür raporların, taciz edici veya uygunsuz internet kullanımının bulunması veya sosyal ağlarda ortak eylem modellerinin karmaşık sistemleri aracılığıyla kimlik bulma durumlarında da kullanılması tavsiye edilir. Çünkü çoğu durumda araştırılan kişinin kimliğine karşılık gelmeyen farklı profiller veya "avatarlar" kullanılmaktadır.

Sonuç olarak, hâkimler ve savcılar, yargılamalarda dijital delil sunma veya sağlama konusunda dikkat edeceklerdir, çünkü her tür dijital ortamda depolanabilen gerçekleri ve/veya bilgileri tespit etmek söz konusu olduğunda güvenlik ve güvenilirlik hususları büyük önem taşıyacaktır.

Bu nedenle, teknoloji uzmanı raporu aşağıdaki unsurları içermelidir:

1. İncelenecek olay veya sürecin tanımı
2. Soruşturma yürütülecek ortamın boyutlandırılması





Bu proje Avrupa Birliđi tarafından
finanse edilmektedir.

3. Elektronik delil toplanması

- (a) Verilerin kurtarılması
- (b) Farklı araştırma tekniklerinin uygulanması

4. Elektronik delillerin muhafaza edilmesi

- (a) Delillerin depolanması
- (b) Etiketleme
- (c) Delil zinciri

5. Delil analizi

- (a) Yeniden yapılandırma
- (b) Cevaplar

6. Belgeleme ve sonuçlar (Uzman raporu)

7. Mahkemede doğrulama ve raporun savunulması

5.4 İyi uygulamalar

A) E-postalar, bilgisayar dosyaları veya bir internet sitesinin içeriđi

Mahkemenin işini ve davacıların teknik yükünü kolaylaştırmak için kağıt formatına dahil edilmelerine halel getirmeksizin dijital [tercihen optik (C-ROM, DVD) veya manyetik (sabit sürücü, USB)] formatta (adli kopya) sunulmalıdır. Adli kopya, uygun deđişiklik yapmayı engelleme protokollerine ve uzman tarafından kendi görüşünde belirtilecek ayrıntılı talimatlara uygun olarak hazırlanacaktır.

Elektronik delil geçiciyse (herhangi bir zamanda gerçekleştirilen bir insan eyleminden dolayı kaybolabilir), en iyi sunum seçeneđi teknoloji izin veriyorsa "dijital noter" aracılığıyla (Avrupa Parlamentosu ve Konseyi'nin 8 Haziran 2000 tarihli 2000/31/EC tarihli Direktifinin gerekliliklerine uyması gereken güvenilir üçüncü taraf) veya uzman liderliğindeki klasik noterin yardımıyla belgelemedir.

B) Mobil cihazlar





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Standart piyasa araçlarının (Cellebrite UFED Touch, Oxygen, Magnet Axiom...) kullanımı aracılığıyla adli tıp uzmanlığı gereklidir ve daha sonra cihazı kendi gözetiminde tutacak olan katibin huzurunda verilerin elde edilmesi için cihazın açılması gerekmektedir. Doğru veri çıkarma, izolasyonu ve iletişim kurulmasını önlemeyi gerektirir, böylece delil bilgisayar uzmanına teslim edildiği andan itibaren değişmeden kalır.

Mobil cihazlarla ilgili olarak, kolayca manipüle edilebilen WhatsApp mesajlarının sürece katkısı özellikle önemlidir, bu nedenle bir zorluk durumunda, gerçekten manipüle edilip edilmediğini bulmayı amaçlayan bilgisayar uzmanı görüşü gereklidir.

5.5 Delil zinciri

Dijital delilin güvenilirliği garanti edilemiyorsa bunun bir faydası yoktur. Bu, hâkimlerin ve savcılarının, delil zincirini delilin elde edilmesinden çoğaltmaya kadar analiz etmesini gerektirecektir.³

- Tanım

Delillerin gerçekliğini, değiştirilemezliğini ve teminatını sağlamayı amaçlayan bir ceza soruşturması sırasında elde edilen delillerin toplanması, aktarılması ve korunmasına yönelik eylemlerin birleşimi olarak tanımlanabilir.

- Mahiyet

Hakimler ve savcılar delil zincirinden haberdar olmak için şunları bilmelidir:

- Neyin alındığı,
- Kimin delile erişim sağladığı,
- Hangi aşamalardan geçildiği,
- Delilin yeniden üretilmesi ve olası kopyalaması,
- Delilin korunması.

Ancak buna rağmen, delil zincirinin elektronik delilin değiştirilemezliğini garanti etmediği açıktır çünkü hem donanım hem de yazılım olmak üzere orijinal cihazların aynı kopyalarını oluşturmaya izin veren birçok araç mevcuttur.

- HASH'e dikkat edilmesi

³ STS 347/12, Haziran 12 "... suç mahallinden toplandığı andan incelendiği ve imha edildiği son ana kadar hareket eden, ölçülen, tartılan ve analiz edilenin her zaman aynı olduğundan tamamen emin olmak gerekir..."





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Elektronik delilin ömrü boyunca (toplanmasından artık doğru olmamasına ve imha edilmesine kadar) değiştirilmemesini sağlayan tek şey, çok küçük bile olsa herhangi bir varyasyonu hesaba katacak olan parmak izi, yani HASH'dir.

6.- Avrupa Konseyi Bakanlar Komitesi'nin Adli ve İdari Yargılamalarda Elektronik Delillere Dair Kılavuz İlkeleri

Burada, kılavuz ilkelere ilişkin kısa bir özet, Açıklayıcı Muhtıradan bazı görüşler ve uygulamaya yönelik bakış açısıyla ek bir girdi sunulmaktadır.

• Arka plan: Avrupa Konseyi, 2016 yılında ADLİ VE İDARİ YARGILAMALARDA ELEKTRONİK DELİLLERİN KULLANILMASI VE BU DELİLLERİN DELİL KURALLARI VE İSPAT USULLERİ ÜZERİNDEKİ ETKİSİNE ilişkin bir rapor hazırlamıştır (Uwe RASMUSSEN'in yardımıyla Stephen MASON tarafından).

Rapor; medeni hukuk, idare hukuku ve ticaret hukuku ile ilgili yargılamalara odaklanarak, elektronik delillerin delil kuralları ve ispat usulleri üzerindeki etkisine göre kabul edilen veya uyarlanan mevcut ulusal yasal hükümlerin karşılaştırmalı bir incelemesini ve analizini kapsamaktadır. Çalışmanın amacı, üye devletlerdeki farklı hukuk sistemlerinin bu alanda karşılaştıkları ve bunlara ilişkin olarak çözüme ihtiyaç duydukları veya bunlarla ilgili çözüm ürettikleri sorunları tespit etmektir.

Raporda şu husus açıklanmaktadır: "Çalışmanın amacı, hakimleri, avukatları ve hukukçuları bu yeni delil biçimine ilişkin bakış açılarını değiştirmenin gerekli olduğunu anlamaya teşvik etmektir. Kağıt üzerine içerik kaydetmek, ortam ve içeriğin birbirine bağlı olduğu anlamına gelir. Dijital bilgi tamamen farklıdır. Temel seviyede, 'bitler ve baytlar' içeriği, yani 0'lar ve 1'leri kapsar. Ayrıca ortam birçok farklı cihaz olabilir ve verileri okumak ve yorumlamak için insanlar tarafından yazılmış bir yazılım gerekir. Bu, kavramsal bir değişim ihtiyacını kavramamız gerektiği anlamına gelir. Benzersiz özellikleriyle, elektronik delillerin bütünlüğü ve güvenliği hakkında karmaşık sorular gündeme gelebilir ancak karmaşık elektronik delil türlerinin doğrulaması e-postalar veya kısa mesajlar gibi daha az karmaşık elektronik delil türlerinden farklı olacaktır".

• Bakanlar Komitesi, gerekçeler bölümünde, Avrupa Konseyi'nin amacının, özellikle hukuki konularda ortak kuralların benimsenmesini teşvik ederek ve adli ve idari yargılamalarda elektronik delillerin işlenmesi için pratik rehberlik sağlayarak üye Devletler arasında daha büyük bir birliği sağlamak olduğunu açıklamaktadır. Farklı üye Devletlerin





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

yasal sistemlerindeki çeşitliliğe saygı göstererek, üye Devletlerin ulusal mevzuatının tam uyumlaştırılması yerine ortak bir çerçeve sağlamayı amaçlamaktadır.

Muhtıra, kılavuz ilkeleri benimseme nedenlerini açıklarken, Avrupa Mahkemelerinin giderek artan bir şekilde elektronik delillerle ilgilenmeye veya taraflar ve adli veya idari yargılamalara dahil olan diğer kişiler tarafından elektronik veri üretimine izin vermeye çağrıldıklarına atıfta bulunmaktadır.

Uluslararası düzeyde, Avrupa düzeyinde veya ulusal düzeyde elektronik delillere çok az standart uygulanabilirken, elektronik delillere uygulanabilecek kanun ve uygulamada önemli eksiklikler devam etmektedir.

Kılavuz ilkelerin amacı, bağlayıcı yasal standartlar oluşturmak değil, Avrupa Konseyi üyesi Devletlere, elektronik delillerle ilgili olarak ortaya çıkan sorunları ele almak için adli ve diğer anlaşmazlık çözüm mekanizmalarının işleyişini uyarlamada pratik bir araç olarak hizmet etmektir. Bu bakımdan kılavuz ilkeler, adaletin etkinliğini ve kalitesini güçlendirmeyi amaçlamaktadır.

Elektronik deliller, birçok bakımdan diğer delil türlerinden farklılık gösterir ve mahkemelerde ve yargılama işlevine sahip diğer yetkili makamlarda elektronik delillerle uğraşırken belirli zorluklar ortaya çıkar. Bu zorluklar, elektronik deliller hakkındaki bilgileri geliştirme ve adli ve idari yargılamalarda elektronik delillerin işlenmesini iyileştirme ihtiyacına işaret etmektedir.

Taslak hazırlama sürecinde, Litvanya (elektronik adalet sistemi ("LITEKO") ve Hırvatistan (e-Ticaret Sicili, e-Tapu Sicili ve entegre bir dava takip sistemi ("espas")) gibi üye Devletlerde mevcut olan elektronik adalet mekanizmalarının işleyişinden gelen deneyimlerden yararlanılmıştır. İspanya'da Mahkemelerle ilişkilerde "sıfır kağıt politikası" vardır ve taraflar ve hukukçular, başvurularını ve belgelerini dosyalamak için elektronik bir platform kullanmak zorundadır ("Lexnet").

Aşağıdaki kılavuz ilkeler yasal olarak bağlayıcı değildir. Amaçları, her ülke kanunu ve içtihadı tarafından belirlenen sınırlar dahilinde elektronik delillerle çalışmak için bazı pratik araçlar önererek adaletin etkinliğini ve kalitesini standartlaştırmak ve güçlendirmektir. Pratik tavsiye niteliğindedirler ve bir "ilkeler beyanı" değildirler.

- Amaç ve kapsam: Kılavuz ilkeler, hem adli hem de idari yargılamalarda uyuşmazlıkların çözümü için geçerlidir. Bu ilkelerin, ticari davaları ve aile davalarını ve her türlü adli incelemeyi içerdiğini varsayabiliriz. Kılavuz ilkelerin konusunu;

Uzaktan ifade alma,

Elektronik delillerin kullanımı,

Delil toplanması, elde edilmesi ve iletimi,

İlgililik,

Güvenilirlik,





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Depolama ve muhafaza,

Arşivleme,

Farkındalık oluşturma, gözden geçirme, öğretim ve eğitim hususları oluşturmaktadır.

Kılavuz ilkeler, hiçbir şekilde bu ilkeler belli tür elektronik delillerin kanıt gücüne haiz olduklarına dair bir kabul getiriyor şeklinde yorumlanmamalı ve yalnızca ulusal mevzuatla çelişmediği sürece uygulanmalıdır. Her üye devletin, hukuk davalarında tipik olarak "olma ihtimali olmama ihtimalinden daha yüksek" ve ceza davalarında "makul şüphenin ötesinde" olan özel ispat yükünde herhangi bir değişiklik yoktur.

6.1 Tanımlar

“Elektronik delil”: İşleyişi bir yazılım programına ya da bir bilgisayar sisteminde veya ağında tutulan veya bu sistem veya ağ üzerinden aktarılan veriye bağlı olan herhangi bir cihaz tarafından oluşturulan veya bu cihaz içerisinde yer alan veriden elde edilmiş her türlü delil.

“Üst veri (metadata)” diğer elektronik verilere ilişkin olup delilin kimliğini, kaynağını veya tarihini belirleyebilmesinin yanında ilgili tarihlerin ve zamanların tespitini sağlayabilme potansiyeline sahip elektronik bilgi anlamına gelmektedir.

“Güven hizmeti”: Aşağıda yer alan unsurları içeren elektronik hizmet:

Elektronik imzaların, elektronik mühürlerin ya da elektronik zaman damgalarının oluşturulması, doğrulanması ve geçerli kılınmaları; kayıtlı elektronik dağıtım hizmetleri ve bu hizmetlere ilişkin sertifikalar ya da internet sitesi doğrulama hizmetleri için sertifika oluşturulması, bu sertifikaların doğrulanması ve geçerli kılınmaları ya da elektronik imzaların, mühürlerin muhafazası veya bu hizmetlere ilişkin sertifikalar.

"Mahkeme": Yargılama yapma yetkisiyle donatılmış ve bu yetkinin icrasında elektronik delillerden faydalanan her türlü yetkili makam. Fakat kılavuz ilkelerde yalnızca hukuk davalarına (ticari davalar ve aile davaları dahil olmak üzere) veya idari davalara atıfta bulunmaktadır.

6.2 Temel prensipler

Bu kılavuz ilkelerin yasal olarak bağlayıcı olmadığını ve uygulanmasının Avrupa İnsan Hakları Mahkemesi'nin incelemesine tabi olmadığını bir kez daha vurgulamak isteriz. Ulusal mahkemelerin egemenliğine saygı duyulur. Elektronik delillerin sahip oldukları potansiyel ispat gücü ulusal mevzuat doğrultusunda mahkemeler tarafından karara bağlanır.

Elektronik deliller; bilhassa delillerin kabul edilebilirliğine, gerçekliğine, kesinliğine ve bütünlüğüne ilişkin hususlar açısından diğer delillerle aynı şekilde değerlendirilmelidir. Gelişen teknolojiye dayalı yeni delil kaynakları olarak görülmektedirler. Ancak davanın esaslarıyla ilgili muhakemeye ve yargısal bulgunun temellerine ilişkin bir ihlal yoktur. Delile ilişkin tüm ilgili içtihat hukuku ve ilkeleri, gerekli düzenlemelerle elektronik delillere uygulanmalıdır.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Elektronik deliller tarafları dezavantajlı bir konuma sokacak ya da taraflardan herhangi birine hâksiz bir avantaj sağlayacak şekilde ele alınmamalıdır. Delillere ilişkin herhangi bir değerlendirme, hem davacı hem de davalı için eşitliği garanti etmelidir. Bu prensip, adli yardımla ilgili soruları gündeme getirir. Böylece çok az kaynağa sahip davacılar, elektronik delil elde etmek veya değerlendirmek için araçlara eşit erişime sahip olabilir. Bu, verileri analiz etmek için bilirkişilerin müdahalesi gerekiyorsa büyük önem taşıyabilir.

6.3 Kılavuz ilkeler

• Uzaktan ifade alma [Kılavuz ilke 1-5]

Delilin niteliği izin veriyorsa, ifade alımı, teknik cihazlar kullanılarak uzaktan yapılabilir. Burada elektronik cihazlar, tarafların, tanıkların veya bilirkişilerin doğrudan, yüz yüze sorgulamasının yerine geçecek bir araç olarak kullanılmaktadır. Ancak delilin kendisi elektronik değildir.

AB düzeyinde, Üye Devlet Mahkemeleri Arasında Medeni Hukuk veya Ticaret Hukuku Meselelerinde Delil Toplanmasına İlişkin İş Birliği Hakkında 28 Mayıs 2001 Tarih ve (AT) 1206/2001 Sayılı Konsey Tüzüğü'nün 10 (4) maddesinde, talep eden mahkemenin talepte bulunulan mahkemeden özellikle video konferans olmak üzere iletişim teknolojisini kullanmasını isteyebileceği belirtilmektedir. Kural olarak, "sanal" sözlü ifadelerin alınması, bir mahkemedeki geleneksel duruşmaya mümkün olduğunca yakın olmalıdır.

Muhtıra, aşırı uzun yargılamalardan kaçınmak için ekonomik hususları (örneğin, ilgili masrafların azaltılması), pratik zorlukları (örneğin, bir tanığın hastalığı, sakatlığı) ve usulün verimli olmasına ilişkin çabaları vurgulamaktadır. Bir kişi farklı bir ülkede ikamet ediyorsa, onu uzaktan sorgulamak daha uygun olabilir. Aynı ilke, davayı gören mahkemenin yargı bölgesinden uzak bir yerde ikamet eden kişilerle de ilgilidir. Bir kişi kilit tanıkta, onu mahkemede sorgulamak daha uygun olabilir. Mahkemeler tarafından dikkate alınması gereken diğer faktörler, tercümanların duruşmaya katılımı ve masraflarıdır. Hakimler, avukatlar ve hukukçular ile mahkeme personelinin yüz yüze ifade ile uzaktan ifade arasındaki olası farklılıkların farkında olması önemlidir. Örneğin, tanıkların tavrını gözlemlemek ve yorumlamak daha zordur.

Mahkemeler, ifade almanın uzaktan yapılıp yapılmayacağına karar verirken (kendi gerekçesiyle veya tarafların talebi üzerine) bilhassa aşağıda yer alan faktörleri göz önünde bulundurmalıdırlar:

- Delilin önemi,
- İfadesi alınacak kişinin statüsü (tanıklar, taraflar),
- Delilin aktarılacağı video bağlantısının güvenliği ve bütünlüğü,
- İfadesi alınacak kişinin mahkeme huzuruna getirilmesinin yol açacağı masraflar ve zorluklar (maliyet-etkinlik analizi).





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Bu bağlamda, COVID-19 küresel salgını, ülkeler arasında ve hatta ülke içindeki şehirler arasında vatandaşların hareketini kısıtlayan tüm halk sağlığı kısıtlamaları ile birlikte dikkate alınması gereken başka bir durumdur. Kırılgan bir durumda bulunan tarafları veya hukukçuları korumak için güvenlik hususları uygulanmalıdır. Tarafların veya tanıkların fiziksel olarak mahkeme önünde olduğu durumlarda uzaktan bağlantıların kullanımına izin vermek geniş anlamda yorumlanabilir ancak avukatların duruşmaya uzaktan katılmak için makul gerekçeleri olmalıdır (aynı ülkede veya yurt dışında). Bu, aynı zamanda bir dijital delil durumu olarak da kabul edilebilir çünkü avukat tarafından yapılan inceleme veya çapraz sorgulama uzaktan bağlantılar aracılığıyla gerçekleştirilecektir.

Gereklikler: Yargılamanın hem taraflar hem de genel kamuoyu tarafından izlenmesine izin verilmelidir. Her durumda, tarafların çapraz sorgulama veya incelemeleri yeniden yönlendirme hakkı garanti altına alınmalıdır. Gizliliğin korunması gereken bazı durumlarda (örneğin, aile davaları), davanın halka açıklığını kısıtlayan aynı kuralların hem elektronik hem de normal delillere uygulanması gerektiğini varsayabiliriz. Delil sunan tarafın veya tanığın, hakkaniyeti garanti altına almak için yargılamanın geri kalanını dinlemesine izin verilmelidir. Yine, mevcut veya uzaktaki tanıklar arasında ayırım yapılmaksızın aynı kurallar geçerli olacaktır.

Teknoloji, dahil olan kişilerin kimliğinin tespit edilmesine izin vermelidir (elektronik olmayan delillerde kullanılanla aynı derecede kesinlik ile). Çocukların (aile davalarında örneğin) veya zihinsel sorunları olan kişilerin sorgulanması ve bunların yaratabileceği zorluklarla ilgili özel bir hüküm yoktur.

Muhtıra, hem kamuya açık hem de özel olmak üzere mevcut tüm iletişim sistemlerinin, dinlenilmeye karşı koruma sağlamak için en azından video konferans kalitesini ve video sinyalinin şifrlenmesini sağlaması gerektiğinin altını çizmektedir. Kullanılan çözümlerin yeterli teknik güvenlik sağlaması ve usul güvencelerini gözetmesi koşuluyla, ulusal hukukun izin vermesi durumunda, özel bir bağlantı yoluyla delil almak mümkündür. Bu bağlamda özel bağlantı, özellikle mahkemede delillerin alınması için oluşturulmuş resmi ve devlete ait olmayan iletişim sistemi anlamına gelir.

Delilin özel veya halka açık bir bağlantı yoluyla iletilmesine bakılmaksızın, video konferans kalitesi sağlanmalı ve video sinyalinin, dinlenilmeye karşı korunması için şifrlenmesi gerekir. Kılavuz ilkeler, mahkeme tarafından tüm koşullar dikkate alınarak karar verilmesi gereken belirli bir şifreleme yöntemi belirtmemektedir.

Elektronik delillerin kullanımı [Kılavuz ilkeler 6-9]

Mahkemeler elektronik delilleri reddetmemeli ve yalnızca elektronik bir formatta toplandıkları ve/veya sunuldukları için yasal olarak haiz olmaları gereken etkiden bu delilleri yoksun bırakmamalıdır.

Kural olarak mahkemeler, yalnızca gelişmiş, kaliteli ve benzeri şekilde güvence altına alınmış bir elektronik imzanın yokluğunu gerekçe göstererek elektronik delilleri yasal olarak haiz olmaları gereken etkiden yoksun bırakmamalıdır. Elektronik sertifikaların veya mühürlerin gerekli olmadığı unutulmamalıdır. Fakat elektronik imzanın veya başka herhangi





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

bir güvenli aktarım biçiminin kullanılması, delillerin ağırlığına ve ikna gücüne büyük ölçüde katkıda bulunur.

Muhtıra, delilleri güvence altına almak için özel olarak kullanılacak bir teknoloji örneği sunar: Blok zinciri, elektronik delillerde daha fazla güven ve güvenlik sağlama potansiyeline sahip olan gelişmekte olan bir teknolojidir. Kriptografi kullanılarak bağlanan ve güvence altına alınan ve merkezi olmayan bir ağda kaydedilen kayıtların (bloklar) listesine atıfta bulunan katılımcılar tarafından bağımsız olarak tutulan ve güncellenen bir veri tabanı olarak tanımlanabilir. Tasarım gereği, bir blok zinciri, verilerin değiştirilmesine doğal olarak dirençlidir. Kaydedildikten sonra, herhangi bir bloktaki veriler, sonraki blokların tümü değiştirilmeden geriye dönük olarak değiştirilemez. Bu, ağ çoğunluğunun gizli anlaşmasını gerektirir. Bu, blok zincirini delil amacı için uygun hale getirir. Ancak bu yalnızca bir örnektir ve kılavuz ilkeler, iletişimin güvenliğini sağlamak için yeni sistemlere açıktır.

Elektronik belgelerin kullanımı söz konusu olduğunda, e-APP'e (elektronik Apostil Programı) atıfta bulunulmalıdır. 2006 Nisan ayında, Lahey Uluslararası Özel Hukuk Konferansı (HCCH) ve Amerika Birleşik Devletleri Ulusal Noterler Birliği (NNA) elektronik Apostil Pilot Programını resmen başlatmıştır. E-APP'nin amacı, (i) elektronik Apostillerin (e-Apostiller) verilmesi ve (ii) alıcıların aldıkları Apostillerin (hem kağıt hem de elektronik) kaynağını doğrulamak için çevrimiçi olarak erişebilecekleri elektronik Apostil Kayıtlarının (e-Kayıtlar) işletilmesi için düşük maliyetli, operasyonel ve güvenli yazılım teknolojisinin uygulanmasının teşvik edilmesi ve buna yardımcı olunmasıdır.

E-APP, Apostil Sözleşmesinin güvenli ve etkili işleyişini daha da geliştirmek için etkili bir araçtır; güvenliği önemli ölçüde artırır ve dolandırıcılığa karşı çok güçlü ve etkili bir caydırıcılık sunar. E-APP teknolojiye bağımsızdır ve belirli bir teknolojinin kullanımına diğerine göre ayrıcalık tanımaz, Akit Taraflar ihtiyaçlarına en uygun teknolojiyi seçmekte özgürdür. E-APP (e-Apostil ve/veya e-Kayıt bileşeni) dünya çapında birçok ülkede uygulanmıştır ve diğer ülkeler de aktif olarak uygulamayı takip etmekte veya düşünmektedir. HCCH, e-APP'nin uygulanmasını tartışmak ve teşvik etmek için düzenli olarak e-APP üzerine Uluslararası Forumlar düzenler. Bunlardan sonuncusu, Özel Komisyon toplantısına denk gelecek şekilde 2016'da düzenlenen 10. Forum olmuştur.

Her halükarda, Apostil'in tek etkisinin (ve aşağıdaki ilke elektronik Apostil'i kapsayacak şekilde genişletilebilir) imzanın gerçekliğini, belgeyi imzalayan kişinin yetkisini ve uygun olduğu durumlarda, belgenin taşıdığı mühür veya damganın kimliğini onaylamak olduğu belirtilmelidir. Apostil, temelde belgenin içeriğiyle (yani apostilize edilmiş resmi belge) ilgili değildir.

Mahkemeler, üst verilerin ispat niteliğindeki değerinin ve bunları kullanmamanın olası sonuçlarının farkında olmalıdır. Bu kılavuz ilke, üst verilerin (diğer elektronik verilerle ilgili elektronik bilgiler anlamına gelir) önemini vurgulamaktadır. Temel verilere eklenen bilgiler üzerinde farklı katmanlar olarak görülebilir ve bu, verileri bağlama oturtmak için çok yararlıdır. Yargı mensuplarına üst verilerle ilgili özel bir eğitim verilmesi tavsiye edilebilir. Aksi takdirde mahkemeler, sağlanan elektronik bilginin değerini anlamak ve değerlendirmek söz konusu olduğunda üst verinin ilgi düzeyi hakkında bilgilendirilmek veya tavsiye almak için bilirkişilere danışabilir.

Tarafların elektronik delilleri çıktı olarak sunmalarına gerek kalmadan orijinal elektronik formatında sunmalarına izin verilmelidir. Pek çok ülke (örneğin, İspanya) adli





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

işlemlerde “sıfır kağıt politikası” nı savunmaktadır, bu da bir adım daha ileri gitmektedir. Çünkü tarafların tüm belgeleri elektronik bir platform kullanılarak dosyalanmalıdır. Bu nedenle basılı kopyalara sadece istisnai olarak izin verilmektedir.

Muhtıra, elektronik delil çıktılarının üst verileri veya diğer gizli verileri hariç tuttukları için kolayca manipüle edilebileceği konusunda uyarmaktadır. Bu, taraf web tarayıcısı ekranından bir çıktı sunduğunda, böyle bir çıktının güvenilir elektronik delil olarak veya uzmanın doğruluk doğrulamasının temeli olarak zorlukla kabul edilebileceği anlamına gelmektedir. Çıktı, ekran görüntüsünün bir kopyasından başka bir şey değildir. Çok basit bir şekilde değiştirilebilir çünkü bu amaç için özel bir yazılım veya donanım gerekmez. Bu nedenle, kural olarak, elektronik deliller orijinal elektronik formatta ve doğruluğunu kontrol etmek için mevcut üst verilerle birlikte sunulmalıdır.

• Delillerin toplanması, elde edilmesi ve iletimi [Kılavuz ilkeler 10-16].

10. Elektronik delil makul ve güvenilir bir metot izlenerek toplanmalı ve bu delillerin mahkemelere ibrazı güven hizmetleri gibi güvenilir hizmetler kullanılarak sağlanmalıdır. Neyin "güvenilir" ve "güven" hizmeti olarak değerlendirilmesi gerektiğine karar vermek için her devlete yeterince alan tanıyan çok kapsamlı bir ilkedir. (Hızla değişen) Belirli bir sistem veya platform lehine karar verilmemektedir.

11. Elektronik delillerin elektronik olmayan delillere nazaran sahip olduğu daha yüksek tahrip olma veya kaybolma riski göz önüne alındığında, üye devletler elektronik delillerin güvenilir bir şekilde elde edilmesi ve toplanmasına ilişkin olarak özel prosedürler geliştirmelidirler. Bu, tarafların kendilerine değil, herhangi bir ülkenin yargı ve idaresine yüklenen bir yükümlülüktür. Kural olarak, ilerlemenin en iyi yolu, yargı dosyalarını bir bütün olarak dijitalleştirmek ve taraflarca sunulan delilleri sisteme dahil etmektir.

12. Mahkemeler, elektronik delillerin yabancı ülke sınırları içerisinde elde edilmesi ve toplanmasına bağlı olarak ortaya çıkması muhtemel sorunların, sınır aşan dosyalardakiler de dahil olmak üzere, farkında olmalıdırlar.

Yurtdışında toplanan kanıtlardan kaynaklanan bir sorun, çeviriler ve elde edilen verilere çevirilerin eklenmesidir. Dikkate alınması gereken bir diğer konu da elektronik çeviri sistemlerinin rolü ve doğruluğudur. Çünkü bu sistemler, yargılama masraflarını olabildiğince düşük tutmak için taraflarca kullanılacak ucuz ve kullanışlı bir araçtır.

Muhtıraya göre, veri kullanımı doğası gereği kesinlikle yerel olabilse de diğer ülkeleri ilgilendiren sınır ötesi bir yapıya sahip olma olasılığı daha yüksek hale gelmektedir. Verilerin işlenmesi veya depolanması için kullanılan altyapının başka bir ülkedeki konumu veya verinin depolanmasını veya işlenmesini sağlayan sağlayıcının konumu buna bir örnektir. Sınır ötesi davalarda mahkemeler ile bulut hizmetleri sağlayıcıları arasında doğrudan iş birliği teşvik edilmelidir. Elektronik delilleri işlerken, hakimler, avukatlar ve hukukçular, hizmet sağlayıcının kuruluş yeri, verilerin işlendiği yer ve verilere erişimi düzenleyen yerel yasaların varlığı gibi faktörleri göz önünde bulundurabilir.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Sınır ötesi teknoloji örneği, veri paylaşımıdır (bulut), farklı fiziksel konumlarda bulunabilecek çeşitli sunucular arasında bir veri tabanının farklı parçalarının depolanmasıdır. Yaygın bir güvenlik tekniği haline gelmiştir. İnternetin küresel doğası ve bulut hizmetlerinin artan kullanımı, verilere erişimin doğası gereği kesinlikle yerel olduğunu varsaymayı giderek zorlaştırmaktadır.

13. Mahkemeler sınır aşan delil toplama durumlarında birbirleriyle işbirliği içerisinde olmalıdırlar. Delil toplanmasına dair kendisine talepte bulunulan mahkeme, talepte bulunan mahkemeyi delilin hangi koşullara bağlı olarak toplanabileceği, bu bağlamda hangi kısıtlamaların söz konusu olduğu hususunda bilgilendirmelidir.

Muhtıra, delil toplanmasına ilişkin ulusal usul kuralları arasında önemli farklılıklar olduğunun farkındadır. Yurt dışında alınan delilleri kullanan mahkemeler bu farklılıkları dikkate almalıdır. Sınır ötesi elektronik delil alımında mahkemelerin bu konuda yakın iş birliği yapması tavsiye edilmektedir. Elektronik delillere ilişkin değerlendirmelerini uygun olduğu durumlarda uyarlamak için talepte bulunulan mahkeme tarafından kullanılan usul kuralları hakkında talepte bulunan mahkeme bilgilendirilmelidir. Özellikle yurtdışında delil toplanması, silahların eşitliği gibi usul hukukunun temel ilke ve haklarının ihlal edilmesine neden olmamalıdır.

Hukuk davalarında delil toplamada adli iş birliği, 18 Mart 1970 Tarihli Hukukî ve Ticarî Konularda Yabancı Ülkelerde Delil Sağlanmasına Hakkında Sözleşmesinin uygulanmasını içerir (Türkiye tarafından onaylanmıştır ve 12-X-2004'ten beri yürürlüktedir). Sözleşmenin amacı, medeni hukuk ve teamül hukuku sistemleri arasındaki farklılıkların üstesinden gelmek için Taraf Devletler arasında medeni veya ticari konularda yurtdışında kanıt toplamak için iş birliği yapmaktır. 1970 yılında imzalandığı için elektronik delillerin alınmasıyla ilgili herhangi bir hüküm bulunmaması şaşırtıcı değildir. Sözleşme, iş birliği için iki yol önermektedir:

İstinabe Talepleri. Talep Eden Devletin yetkili makamı, İstinabe Talebini Talep Edilen Devletin Merkezi Makamına [Türkiye'de, Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü'ne] iletir. Merkezi makam daha sonra İstinabe Talebini talep edilen devletin iç hukukuna göre icra edilmek üzere ülkesindeki yetkili makama iletir. Ne mektubun iletimi ne de yurtdışında kanıt toplanması dijital delillerle ilgilidir.

Diplomatik memurlar, konsolosluk görevlileri veya özel memurlar (önceden izne tabidir veya talep edilen Devlette hariç bırakılır). Bu memurlar, talebi yerine getirecek Devletin kanunlarına uygunsa delil alabilir ve ayrıca bir yemin veya onaylama yetkisine de sahip olabilir. Diplomatik memurlar, konsolosluk görevlileri veya özel memurlar, talep edilen kişiyi ifade vermeye zorlayamaz.

Belgelerin duruşma öncesi ortaya çıkarılması (bir iddianın sunulmasından sonra ancak esasa ilişkin nihai duruşmadan önce sunulan delil taleplerini kapsayan, teamül hukuku ülkelerinde tipik usul). Sözleşme, Taraf Devletlere, beyanda bulunmak suretiyle, belgelerin duruşma öncesi ortaya çıkarılması amacıyla İstinabe Taleplerinin, bir tarafın yalnızca diğer tarafın elinde hangi belgelerin içinde bulunabileceğini bulmaya çalıştığı taleplerden kaçınmak için yeterince doğrulanmasını sağlamalarına izin vermektedir. Rekabet hukuku davaları gibi belirli dava alanlarında çok ilgili ve yaygın olan elektronik delillerin toplanmasına ilişkin herhangi bir hüküm bulunmamaktadır.

AB içinde, ilgili kurallar, Üye Devlet Mahkemeleri Arasında Medeni Hukuk veya Ticaret Hukuku Meselelerinde Delil Toplanmasına İlişkin İş Birliği Hakkında 28 Mayıs 2001





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

Tarih ve (AT) 1206/2001 Sayılı Konsey Tüzüğü tarafından sağlanmaktadır. Belgenin eksikliklerinden biri, elektronik delillerin toplanması ve kullanılmasıyla ilgili özel hükümlerin bulunmamasıdır.

Mahkemeler arasında doğrudan aktarım yoluyla iş birliği çalışmaları: Talepler, yargılamanın başlatıldığı veya tasarlandığı mahkeme tarafından (bundan böyle 'talep eden mahkeme' olarak anılacaktır) doğrudan başka bir Üye Devletin yetkili mahkemesine delil toplamanın gerçekleştirilmesi için iletilir. Her Üye Devlet, delil toplama görevini üstlenen mahkemelerin bir listesini hazırlayacaktır (bu mahkemelerin bölgesel ve özel yargı yetkisi).

Merkezi makam: Her Üye Devlet; mahkemelere bilgi sağlamak, bir taleple ilgili olarak ortaya çıkabilecek herhangi bir zorluğa çözüm aramak gibi görevleri olan bir merkezi makam belirleyecektir.

Talebin biçimi ve içeriği: Talep, Form A veya uygun olduğu durumlarda Ek'teki Form I kullanılarak yapılacaktır. Talep şu hususları içerecektir: (a) talepte bulunan ve uygun olduğu hallerde talep edilen mahkeme; (b) yargılamanın taraflarının ve varsa temsilcilerinin isimleri ve adresleri; (c) davanın niteliği ve konusu ve olayların kısa bir açıklaması; (d) gerçekleştirilecek delil toplama işleminin bir açıklaması; (e) talebin bir kişinin sorgulanması durumunda: sorgulanacak kişi(ler)in adı(ları) ve adres(ler)i, sorgulanacak kişi(ler)e sorulacak sorular veya sorgulanması gereken olguların beyanı, uygun olduğu hallerde, talepte bulunan mahkemenin Üye Devletin kanunları uyarınca ifade vermeyi reddetme hakkına atıf, incelemenin yapılması gerektiğine dair herhangi bir şart, yeminle veya bunun yerine onay ve uygun olduğu durumlarda kullanılacak herhangi bir özel form, talepte bulunan mahkemenin gerekli gördüğü diğer bilgiler; (f) talebin başka herhangi bir delil toplama şekli olması durumunda, incelenecek belgeler veya diğer nesneler.

Elektronik iletişim araçlarının kullanımı Tüzükte ele alınmamaktadır. Ancak farklı Üye Devletlerin Mahkemeleri arasında talepleri iletmenin bir yolu olarak e-posta yaygın kullanılan bir araçtır. Sözlü delillerin alınması için video konferanslar yapılması, davayı büyük ölçüde kolaylaştırabilir, tarafların talep edilen mahkeme tarafından delil toplama anında hazır bulunma hakkı gibi tüzük hükümlerinin çoğunu gereksiz hale getirebilir. Ve soruları cevaplamayı reddetme ayrıcalıkları olduğu iddia edilen tanıklarla ilgili kararlar. Deliller uzaktan bağlantılarla alınırsa, tüm bu konular talepte bulunan Mahkeme tarafından iç mevzuat uygulanarak daha etkin bir şekilde çözülebilir.

Üye Devletlerdeki merkezi makamlar, Tüzük hükümlerinin yanı sıra Avrupa Konseyi Kılavuz İlkelerinin uygulamasını teşvik etmek için kullanılabilir.

14. Elektronik deliller, delillerin başka mahkemelere iletilmesini kolaylaştıracak şekilde toplanmalı, düzenlenmeli ve ele alınmalıdır. Yine, sadece delilleri değil, tarafların tüm yazılı görüşlerini, dilekçelerini, önermelerini ve Mahkeme'nin ara, usul ve nihai kararlarını içeren bir elektronik dosyanın kullanılması, bu amaca ulaşmanın en iyi yoludur.

15. Dava sürecinin daha etkin bir şekilde işleyebilmesine yardımcı olmak adına elektronik delillerin iletiminin elektronik araçlar vasıtasıyla yapılması teşvik edilmelidir.

Muhtıraya göre, iletilen elektronik verilere üst veriler eşlik etmelidir. Bu, uygun veri yönetimi amaçları için mahkemeler tarafından oluşturulan ek üst verilerin kullanımını ve diğer mahkemelere sorunsuz bir şekilde iletilmesini içerir. Yapılandırılmış üst verilere sahip olmak





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

mahkemelere deliller üzerinde kontrol sağlar. İdeal olarak başka bir mahkemeye iletmek için elektronik delillerin bir kopyası kullanılmalıdır.

Elektronik delillerin elektronik yollarla iletilmesinin teşvik edilmesi ve kolaylaştırılması, ortak teknik standartların, dosya formatlarının uygulanması ve yerel adli ve idari sistemlerin dijitalleştirilmesi yoluyla sağlanabilir. Elektronik delillerin imha riskinin daha yüksek olduğu göz önüne alındığında, elektronik delillerin güvenli bir şekilde iletilmesine izin veren yerel prosedürler benimsenmelidir.

16. Elektronik delillerin iletiminde kullanılan sistemler ve cihazlar bu delillerin bütünlüğünü muhafaza edebilecek nitelikte olmalıdırlar. Kılavuz ilkeler, dosyaların belirli bir şifreleme sistemini savunmamakta, durumlara daha uygun gördükleri sistemleri kullanmaları ve sürekli güncellenen teknolojiye değişikliklere izin vermeleri için yeterli alan sağlamaktadır.

Muhtıra, verilerin korunmasına ilişkin ayrıntılı bilgi vermektedir: Elektronik delil, doğası gereği hassastır ve yanlış kullanım veya inceleme ile değiştirilebilir, zarar görebilir veya yok edilebilir. Bu nedenlerle, bu tür delilleri uygun şekilde toplamak için özel önlemler alınabilir. Bunu yapmamak, onu kullanılamaz hale getirebilir veya yanlış bir sonuca yol açabilir. Prensip olarak taraflar, adli ve idari yargılamalarda elektronik delillerin uygun şekilde toplanmasından sorumludur. Farklı veri türleri, farklı toplama yöntemleri gerektirebilir. Elektronik delilleri güvence altına almak ve toplamak için alınan önlemler, bu delilin bütünlüğünü etkilememelidir. Büyük önem taşıyan konularda, taraflar elektronik delilleri bir bilgisayar uzmanının veya noter hizmetlerinin desteğiyle toplamayı değerlendirmelidir. Hakimler, avukatlar ve hukukçular verilerin genellikle ağ tabanlı hizmetlerle depolandığı hakkında bilgi sahibi olmalıdır. Buna hem bulut bilişim sistemi hem de hizmetlerin çevrimiçi olarak sunulması dahildir.

Bu bağlamda, Bakanlar Komitesinin üye devletlere yargı alanında elektronik belgelerin arşivlenmesi hakkında Rec (2003) 15 sayılı Tavsiye Kararı (Bakanlar Komitesince, Bakan Vekillerinin 9 Eylül 2003 tarihli 851. Toplantısında kabul edilmiştir), bazı genel hükümler sunmaktadır. Üye devletler, arşivleme hususunu düzenleyen hukuk normlarının elektronik belgelere de uygulanmalarını sağlamalıdırlar. Elektronik belgeler bütünlükleri, mevsukiyetleri, güvenilirlikleri ve uygun olduğu hallerde gizlilikleri korunacak şekilde arşivlenmelidir. Arşivlenen elektronik belgelerin okunabilirliği ve erişilebilirliği zaman içinde, bilgi teknolojisindeki ilerleme dikkate alınarak güvence altına alınmalıdır. Basılı belgelerin arşivlenmesinde olduğu gibi, elektronik belgeleri saklama süresi ile bunların halka açılma zamanlarına arşiv sorumlularıyla birlikte karar verilmelidir. Arşivlenen elektronik belgeler, diğer elektronik, basılı veya analog belgelere bağlantının yanı sıra belgelerin oluşturulma gereklerini açıklayan standart üst bilgilerle ilişkilendirilmelidir.

Standartlaştırılmış, birleşik elektronik adli dosyaların kullanılması, verilerin korunmasına yardımcı olabilir, elektronik belgeleri sistemlere entegre edebilir, böylece dosyaları korumak ve yedeklemek için kullanılan aynı cihazlar delillerin depolanmasında kullanılabilir.

Muhtıra, delillerle ilgilenen hukukçular da dahil olmak üzere, hakimlerin ve avukatların, bilgi ve uzmanlık alanlarında bir artış olduğunu ancak belirli standartların hala eksik olduğunu kabul etmektedir. Elektronik delillerin toplanması ve bunlara el konulması, üye Devletler tarafından özel araç ve prosedürlerin benimsenmesini gerektirebilir. Bu arada, hakimler, avukatlar ve hukukçular bu tür verilerin bütünlüğünü, gizliliğini ve güvenliğini sağlamaya çalışmalıdır. Bu, depolama araçlarından birinin başarısız olması durumunda





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

güvenli yedek kopyaların saklanması içerir. Elektronik verilerin orijinal formatlarında tutulması gereklidir.

• İlgililik [Kılavuz ilkeler 17 ve 18]

17. Mahkemeler, bilhassa elektronik delillerin gereğinden fazla ve şüpheli temininin ve bu delillere gereğinden fazla ve şüphe uyandıracak şekilde talebin oluşmasının önüne geçmek amacıyla elektronik delillerin yönetiminde aktif rol almalıdırlar. Kılavuz ilkeler, gereksiz olabilecek veya veri koruma ve mahremiyetle ilgili sorunlar ortaya çıkabilecek büyük miktarda veri ve üst veri toplama riskinin farkındadır. Hakimler yalnızca elektronik delillerin kullanımına izin vermek için değil, aynı zamanda bunların kötüye kullanılmasını önlemek için proaktif bir yaklaşım benimsemelidir.

Muhtırada şöyle açıklanmaktadır: Gereksiz büyük miktarlarda elektronik veri, bir taraf tarafından kolaylıkla sağlanabilir ve bu da mahkemenin ve diğer katılımcıların verileri etkili bir şekilde işlemesini zorlaştırabilir veya imkansız hale getirebilir. Bu nedenle, sunumunu davaya karar vermek için kesinlikle gerekli olanla sınırlamak amacıyla mahkeme tarafından elektronik delillerin aktif yönetimi esastır. Verilerin aktif yönetiminde orantılılık ilkesi gözetilmelidir. Elektronik delil üretmeye yönelik her talebin esasları, özellikle ispat amaçlı yararlılığı dikkate alınmalıdır. Taraflar, bu tür taleplere itiraz etme hakkına sahip olmalıdır. Yine, usule ilişkin kurallara göre, yargılamanın seyri dikkate alınarak hangi kararların temyize tabi olabileceğine karar vermek her ülkenin kendi sorumluluğundadır.

18. Mahkemeler, özellikle delillerin ispat gücüne ilişkin olarak ortaya atılan veya elektronik delillerle oynandığına dair bir iddianın varlığı halinde elektronik delillerin uzmanlar tarafından incelenmesini isteyebilir. Bu uzmanların ilgili konu dahilinde yeterli tecrübeye sahip olup olmadıkları mahkemeler tarafından karara bağlanmalıdır.

Muhtıra, hakimlerin, avukatların ve hukukçuların olası teknik uzmanlık ihtiyacının farkında olmaları ve uzman görüşü gibi daha fazla araştırma veya ek uzman bilgisinin gerekli olabileceği durumlarda bunu kabul etmeleri gerektiğini belirtmektedir. Uzmanlar yetkin olmalı ve verilen görevi yerine getirmek için yeterli eğitime sahip olmalıdır.

Yine, delillerin değerlendirilmesi için yargılamaya hangi tür uzmanlıkların dahil edilmesinin uygun olduğuna karar vermek esas olarak tarafların veya Mahkemenin sorumluluğundadır. Her hâkimin bireysel uzmanlığına ilişkin sorular ortaya çıkmaktadır çünkü yargı içinde yaş, deneyim ve önceki eğitim dikkate alındığında büyük farklılıklar olacağı tahmin edilmektedir.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

7.- Avrupa Soruşturma Emri aracılığıyla diğer ülkelerden nasıl elektronik delil talep edilir? (Karşılıklı Adli Yardımlaşma-Karşılıklı Adli Yardımlaşma Talebi)

Hâkim ve savcılar tarafından bu tedbirin talep edilmesi halinde, aşağıdaki hususların belirlenmesi faydalı olacaktır:

- Ülkenizdeki Operatör/Servis Sağlayıcıyı gösteren IP numarasının belirlenmesi.
- Yukarıda belirtilen IP'ye sahip bilgisayarın bulunduğu yerin adres kaydı. Mümkünse, yerinde bir bilgisayar çalışması yapılması, resim indirme programlarının, bağlantıların ve resim depolamasının, e-posta dahil araştırılması gereken dosyaların kontrol edilmesi.
- Sabit Diskin müteakip incelemesi, talepte bulunulan makam tarafından belirlenen uzmanlar için önemliyse, bunun bir dökümü yapılır ve tüm içeriği, klasörleri vb. bulmak için çalışma yapılır. Soruşturma için faydalı olabilecek içerik hakkında bilgi sahibi olmak için uzmanlar veya adli polis tarafından daha fazla çalışma yapılması için CD, DVD, flaş disk, harici sabit diskler gibi herhangi bir yığın depolama cihazının incelenmesi. Sabit disk vb. çalışmaların yapılmasının mümkün değilse ve talepte bulunan makama iletilmeleri istenirse, delil zincirinin sağlanması için gerekirse polis memurları atanır. Bu polis memurları, transferi devralmak için talebi yerine getiren Devlete gider.
- Ayrıca faillere ve soruşturmada daha sonradan ortaya çıkabilecek diğer kişilere karşı ceza davasında delil olarak bu adli yardım talebiyle elde edilen delilleri kullanabilmek için uygun olduğu hallerde, talebi yerine getiren devlete izin vermenin bu devletin lehine olup olmadığının belirtilmesi. E-posta hesapları hakkında bilgi talep edilmesi durumunda, e-posta hesabındaki mesajların bir kopyasının (hangi mesajların olduğunu veya tarihlerin belirtilmesi) ve alıcılarının veya gönderenlerinin belirtilmesi ile bu mesajların eklerinin bulunması ve iletilmesi. Ayrıca uygun olduğu hallerde, istenen e-posta adresiyle ilgili verilerin saklanması talep edilir.



GERÇEK DAVALAR VE TARTIŞMAYA YÖNELİK FİKİRLER

2.1 DAVA A (Nagla)

Nagla bir yapımcı, muhabir ve araştırmacı bir haber televizyonu programının sunucusuydu. Kendisine "Neo" adını veren bir kişiden, Devlet Gelir İdaresi tarafından tutulan bir veri tabanında ciddi güvenlik açıkları (Elektronik Beyan Sisteminde depolanan verilere erişimi mümkün kılan güvenlik açıkları) olduğunu ortaya koyan bir e-posta almıştır. Yetkililere olası bir güvenlik ihlali hakkında bilgi vermiştir.

Gazeteci olarak görev yapan Nagla, 14 Şubat 2010 tarihinde yayın sırasında Devlet Gelir İdaresi'nden büyük bir veri sızıntısı olduğunu duyurmuştur. "Neo", Twitter hesabı üzerinden merkezi düzeyde ve belediye düzeyinde çeşitli kamu kurumlarında ödenen maaşlara ilişkin verileri yayımlamaya başlamıştır.

Veri sızıntısı ile ilgili olarak ceza davası açılmıştır. Bir polis memuru, Nagla'nın evinde acil bir arama yapıldığını soruşturma hakimine bildirmiştir. Birlikte ele alınan ceza davalarında, suçun işlendiği sırada Nagla'nın şüpheliyle sık sık iletişim kurduğu ve muhtemelen EDS XML dosyalarının yasa dışı indirilmesiyle bağlantılı olarak şüphelinin yasa dışı faaliyetleri ve ayrıca bu dosyalarda, suç ortaklarının ve ceza davasıyla ilgili diğer bilgilerin işlenmesi, depolanması ve dağıtımı hakkında bilgi olabileceği sonucuna varılmıştır.

11 Mayıs 2010'daki arama sırasında, şu veri depolama cihazlarına el konulmuştur: kişisel bir dizüstü bilgisayar, harici bir sabit disk, bir hafıza kartı ve dört flaş disk. Nagla'ya göre, bu cihazlar kişisel verilerinin büyük bir bölümünü ve işle ilgili materyallerinin çoğunu içeriyordu.

Soruşturma hakimi, Nagla'nın evinde ele geçirilen veri depolama cihazlarının teknik incelemesine ilişkin talimat vermiştir. Hükümete göre, tüm bu cihazlar iki adet mühürlü poşet içinde Eyalet Polisi bünyesindeki ilgili inceleme birimine teslim edilmiştir.

Bu poşetler, bir uzmanın onları açtığı 17 Mayıs 2010 tarihine kadar kapalı kalmıştır; ambalajları veya mühürleri zarar görmemiş. Uzman, 17 ve 18 Mayıs 2010 tarihlerinde, veri depolama cihazlarındaki tüm bilgileri özel bir yazılım programı kullanarak başka bir bilgisayara kopyalamıştır. 19 Mayıs 2010'da poşetleri mühürlemiş ve soruşturma hakimine geri vermiştir. 21 Mayıs 2010 tarihinde, veri depolama cihazları başvurana iade edilmiştir.

15 Haziran 2010 tarihinde teknik inceleme tamamlanmış ve Hükümete göre kopyalanan bilgiler imha edilmiştir.

Tartışmaya yönelik bazı fikirler:



Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

- Bu davada, sorunların büyük bir kısmının, siber suç ve dijital delillerin aranması ve depolanması ile ilgili olarak ele alınması gerektiğini düşünüyoruz. Bu bir ceza davası olmasına rağmen, adli ve idari yargılamalarda elektronik delillere ilişkin Avrupa Konseyi Bakanlar Komitesi Kılavuz İlkeleri çerçevesinde bir analiz gerektiren bazı temel haklar ve genel ilkeler mevcuttur.
- Eyalet İlk Derece Mahkemesi, soruşturma hakiminin kararını şu gerekçelerle onamıştır: "Mevcut ceza davası, elektronik ortamda doğrudan bilgi alışverişiyle ilgili gerçeklerle bağlantılı olarak açılmıştır ve bu nedenle, bu tür delillerin çok hızlı bir şekilde değiştirilebilmesi veya yok edilebilmesi nedeniyle, delillerin elektronik biçimde saklanması, elde edilmesi ve kaydedilmesinin hassas olduğu siber suçun belirli özellikleri ile suçun cürmü kastını da hesaba katmak önemlidir."
- Davada farklı temel haklar dikkate alınmalıdır:
 - Bilgi edinme özgürlüğü (bir kamu kurumunun kişisel verileri tutmadaki başarısızlığını ifşa etmek). Ve gazetecinin kaynaklarını gizli tutma hakkına sahip olması. Sözleşmenin 10. maddesi.
 - Gazetecinin aile ve özel hayatına saygı hakkı. Sözleşmenin 8. maddesi.
 - Adil yargılanma hakkı (sanığa karşı kullanılacak, sanık dışında bir üçüncü taraftan delil toplanması).
- Elektronik delillerin toplanması, ele geçirilmesi ve iletilmesi. Bazı noktalar vurgulanmalıdır. AİHM, "soruşturma makamlarının geniş kapsamlı bir arama emrine dayanarak başvuran gazetecinin evini aradıkları gerçeğini" belirtmiştir.
 - Dijital delillerin toplanması, dizüstü bilgisayarlar, tabletler, cep telefonları gibi verilerin depolandığı fiziksel cihazlara daha önce el konulmasını içerebilir. Bu cihazlar bir evde bulunabilir. Bu da mahremiyetle ilgili sorunları ortaya çıkarır.
 - Bilgilerin uygun ve güvenli bir şekilde toplanması ve sunulması, bu cihazların güvenliğinin sağlanması açısından da önemlidir (mühürlü poşetlere konuldular ve daha sonra kopyalanmak üzere açıldılar).
 - Elektronik delillerin ve ayrıca depolandığı cihazların potansiyel olarak yok edilmesi veya kaybolması riski vardır. Elektronik delillerin güvenli bir şekilde ele geçirilmesi ve toplanmasına yönelik prosedürlerde, verileri yok edilmekten korumak ve daha fazla incelemeye izin vermek için cihazların içeriğinin tam yedeklerini almanın kolaylığı düşünülmelidir.
 - Bu davada, verilerin tam olarak hangi bölümünün analiz edildiğini doğrulama şüphesi olmadan, "kopyalanan bilgiler yok edilmiştir". Ancak "Elektronik delillerin işlenmesi taraflar için dezavantajlı olmamalı veya içlerinden birine haksız avantaj sağlamamalı" ilkesi gözetilmelidir.





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

- Soruşturulan suçla hiçbir ilgisi olmayan kişisel elektronik veri miktarı (kişisel videolar veya resimler) ile ilgili olarak ortaya çıkan belirli sorunlar. Bu davada "cihazlar, kişisel verilerinin büyük bir kısmını ve işle ilgili materyallerinin çoğunu içeriyordu".
- Ayrıca analiz edilen verilerin, soruşturma altında olanlardan tamamen farklı olarak başka suçların keşfedilmesine yol açma olasılığını da düşünmeliyiz. AİHM, "ele geçirilen veri depolama cihazlarının, yalnızca bilgi kaynağını tanımlayabilen bilgileri değil, aynı zamanda bilgi kaynağından "bilgi edinmenin gerçek koşullarına" veya bu bilginin "yayınlanmamış içeriğine" ilişkin bilgileri de içerdiğini" onaylamaktadır.
- İlgililik: Kılavuz ilkelere göre, Mahkemeler, özellikle elektronik delillerin aşırı veya spekülatif olarak sağlanmasından veya talep edilmesinden kaçınmak için elektronik delillerin aktif yönetimine katılmalıdır.
 - Bu ilke, soruşturma açısından önemli olan cihazların sayısına da uygulanmalıdır (eğer arama izin daha spesifik ise, bir evdeki tüm elektronik cihazlar veya sabit diskler toplanmalı mıdır?)
 - AİHM, "arama emrinin, kimliğinin soruşturma makamları tarafından önceden bilinmesine bakılmaksızın, gazetecinin kaynağı tarafından işlendiği iddia edilen soruşturma kapsamındaki suçla ilgili "herhangi bir bilginin" ele geçirilmesine izin verecek kadar muğlak terimlerle hazırlandığını" belirtmiştir.
 - Kişisel görünen ve herhangi bir cezai menfaat sağlamayan tüm elektronik veri ve bilgiler mümkün olan en kısa sürede veri sahibine verilmeli ve suç dosyalarından çıkarılmalıdır.
 - Yine üst verilerin öneminin altı çizilmelidir. E-postaların tarihleri ve detayları, arşivlere erişim vb. verilerin kendisi kadar önemli olabilir ve uygun analizlerin alınması gerekir. AİHM, "Hükümet, başvuranın evinde yapılan aramanın "soruşturma altındaki suçla ilgili bilgi" toplamayı amaçladığını ve yalnızca dosyaların kendilerine el konulmasına değil, aynı zamanda bu dosyaların alınmasıyla ilgili bilgilerin (üst veriler) elde edilmesiyle yetkili olduğunu" belirtmiştir.
 - Özellikle karmaşık delil sorunları ortaya çıktığında veya elektronik delillerin manipüle edildiği durumlarda, uzmanlar tarafından elektronik delillerin analizi. Bu davada, "soruşturma hakimi, veri depolama cihazlarının teknik incelemesine yönelik talimat vermiştir ... Eyalet Polisi bünyesindeki ilgili inceleme birimine teslim edilmiştir". Yargılamaya dahil olan tarafların diğer bilirkişiler tarafından kendi incelemelerine devam etme olasılığı göz önünde bulundurulmamıştır.

Olaylar ve alıntılar, Avrupa İnsan Hakları Mahkemesi'nin 16 Temmuz 2013 tarihli NAGLA ve LETONYA Davası Kararından (Dördüncü Bölüm) alınmıştır. Dava, bir başvurudan kaynaklanmıştır (no. 73469/10).





Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

[https://hudoc.echr.coe.int/eng#{\"fulltext\":\[\"73469/10\"\],\"documentcollectionid2\":\[\"GRANDCHAMBER\"\],\"CHAMBER\"\],\"itemid\":\[\"001-122374\"\]}](https://hudoc.echr.coe.int/eng#{\)

2.2 DAVA B (Elektronik delil ve zehirli ağacın meyvesi de zehirlidir teorisi)

İspanya Yüksek Mahkemesinde (Ceza Dairesi, Bölüm 1a, No16 / 30 Ocak 2019), sanığın kendisini mahkum edebilecek elektronik delil araçlarının hukuka aykırı olarak elde edilmesi nedeniyle beraat ettiği bir dava bulunmaktadır. Yüksek Mahkeme, kararının herhangi bir yerinde "zehirli ağacın meyvesi de zehirli olur teorisine" açıkça bir atıfta bulunmazken, dosyada çözülen dava gibi davalarda bu teorinin pratikte uygulanması üzerine düşünmeye davet etmektedir.

Özet

Ulusal Mahkeme (Ceza Dairesi, Üçüncü Bölüm), Ulusal Polis Teşkilatı yetkilisi Fructuoso Gonzalo'yu, ortak rüşvet suçundan cezai olarak sorumlu tutarak mahkum etmiştir. Dört yıl hapis cezası, 45.000 Euro para cezası, dokuz yıl altı aylık bir süre için istihdam veya kamu görevinden men etme ve ortaya çıkan masrafların ödenmesi cezalarını vermiştir.

Fructuoso Gonzalo, uyuşturucu kaçakçılığından hüküm giymiş iki kişiyle (Domingo Ruperto ve Ildefonso Nazario) cep telefonundan gönderilen SMS'ler ve e-posta hesabından gelen e-postalar aracılığıyla, iş birliği yapabilmek için onları bir narkotik kaçakçılığı operasyonuna dahil etmekle suçlanmıştır. Bu bağlamda, Gonzalo, Ildefonso Nazario'ya davasıyla ilgili polis soruşturmalarının durumu hakkında bilgi vermesi karşılığında bir miktar para talep etmiştir. Gonzalo, konumu gereği, teklifin yukarıda belirtilen alıcıları hakkında bilgi sahibi olmadan bu bilgilerden haberdar olmuştur.

Polis, Fructuoso Gonzalo'nun, hayali bir e-posta hesabı (Hugo Fructuoso) aracılığıyla e-postaları yukarıda belirtilen iki kişiye göndermek için internete bağlandığı "IP'yi (İnternet Protokolü)" (Pontevedra'da bulunan bir internet kafe) belirlemiştir.

Domingo Ruperto, Fructuoso Gonzalo'nun para talebine yanıt olarak, ona 30.000 Euro'yu nakit olarak verecekti. Teslimat gününde Fructuoso Gonzalo, Pontevedra tren istasyonunda Europcar'dan kiraladığı, kimliği tam olarak belirlenmiş bir araçla gelmiştir. Domingo Ruperto, talimatlarını uygulayarak, ona, Fructuoso Gonzalo tarafından alınacak miktarla aynı miktarda paranın olduğu bir zarfı arabanın içine bırakmıştır. Domingo Ruperto sadece Fructuoso Gonzalo'yu "Görünmez" olarak biliyordu ve Europcar'dan kiralanan aracın verilerini yazmayı başarmıştır.



Tartışmaya yönelik sorular:

Hangi deliller ve elektronik deliller ve kaç tane delil var?

Yukarıdaki davada Ulusal Mahkeme'nin Fructuoso Gonzalo'yu mahkum etmesine yol açan belirleyici elektronik deliller aşağıdaki gibiydi:

- 1) Polis merkezinde ve genel kurulda Domingo Ruperto ve Ildefonso Nazario'nun verdiği ifadeler.
- 2) Ildefonso Nazario ve Fructuoso Gonzalo arasında olduğu iddia edilen 44 e-postanın içeriği (elektronik delil 1).
- 3) Fructuoso Gonzalo'nun e-postaları yukarıda belirtilen kişilere göndermek için internete bağlanacağı yerin (Pontevedra'da bulunan bir internet kafe) IP bağlantısı (elektronik delil 2).
- 4) Microsoft tarafından sunulan, e-postaları ve içeriklerinin transkripsiyonunu içeren CD (elektronik delil 3).
- 5) Domingo Ruperto ve Fructuoso Gonzalo arasında olduğu iddia edilen SMS'ler (elektronik delil 4).
- 6) Microsoft tarafından iletilen CD'nin içeriğini analiz eden bilgisayar uzmanı raporu (elektronik delil 5).
- 7) Belirli telefon hatlarından gönderilen ve alınan SMS'leri analiz eden bilgisayar uzmanı raporu (elektronik delil 6).
- 8) Microsoft'un Fructuoso Gonzalo, Domingo Ruperto ve Ildefonso Nazario'ya gönderilecek e-postalarda yer alan verilere ilişkin raporu (elektronik delil 7).
- 9) Gonzalo Fructuoso'ya ait olduğu iddia edilen e-posta hesabının IP bağlantı verilerine ilişkin telefon raporları (elektronik delil 8).

Yüksek Mahkeme'nin Ceza Dairesinin kararına ilişkin özet ve kısa açıklama:

Yüksek Mahkeme, Fructuoso Gonzalo'nun Ulusal Mahkeme'nin kararına karşı bir temyiz başvurusunda bulunduğunu ve bu karara binaen, yasaya uygun olarak başka bir karar vererek bu kararı geçersiz kıldığını açıklamıştır.

1) Bir sanığın e-postalarını rızası olmadan analiz etmek mümkün mü?

E-posta kullanıcıları tarafından verilen izin (önceden adli izin olmaksızın), başka bir kişiyi etkilese bile geçerlidir.

Ildefonso Nazario'nun önceden adli izin olmadan, Fructuoso Gonzalo'yla yaptığı yazışmaların doğrulanması için e-postasına erişim sağlanmasına ilişkin polise verdiği izin, Yüksek Mahkeme için söz konusu kişinin "rızası" anlamına gelmektedir. Bu da haberleşmelerin gizliliğine müdahale ve bu hakkın etkilenmesi anlamına gelmemektedir. Bu nedenle, Avrupa İnsan Hakları Mahkemesi'nin şu kararları bu davada uygulanmaz: hepsi haberleşmelerin



Bu proje Avrupa Birliği tarafından
finanse edilmektedir.

gizliliğiyle alakalı olan 24.2.90 tarihli Kostowski ve Fransa davası, 5.11.2002 tarihli Allan ve Birleşik Krallık davası, 8.4.2003 tarihli M.M. ve Hollanda davası.

2) Polis, IP talep etmek için telefon şirketleriyle iletişime geçmek amacıyla adli izin talep etmeli midir?

Polisin doğrudan internete ve mobil şirketlere talepte bulunmak için adli izin alması gerekir.

Mahkeme, Polis tarafından doğrudan Microsoft (Fructuoso Gonzalo, Domingo Ruperto ve Ildefonso Nazario arasında yapılan yazışmalara ve Gonzalo'nun IP bağlantılarına ilişkin verilere erişim ve bunlardan verilere erişim) ve Telefónica (Fructuoso Gonzalo'ya ait olduğu iddia edilen e-posta hesabına ilişkin IP bağlantıları hakkında rapor) şirketlerine yapılan taleplerin yasa dışı deliller olduğunu çünkü bu taleplerin ilgili adli izin alınmadan yapılmış olabileceğini düşünmektedir (davada önceden adli izin belgelenmemiştir). Bu, talimatların hükümsüz ve yasa dışı olarak alınması ve e-postalara ve ilgili verilere müdahale edilmesi anlamına gelir.

3) Bir IP almak ve bunu adli sürece dahil etmek için adli izin gerekli midir?

IP bağlantılarını almak için adli izin almak gereklidir.

4) Bilirkişi raporuna ek olarak, bilirkişiler ifade vermeli midir?

Teknoloji uzmanı raporunun kim tarafından hazırlandığı duruşmada belirtilmelidir.

Yüksek Mahkeme ayrıca Fructuoso Gonzalo'ya ait olduğu iddia edilen e-posta hesabı ve belirli bir IP adresinden bağlantıları ile verilerin elde edilmesinin hukuka aykırı olduğunu düşünmektedir çünkü temyiz edilen kararda;

- Sunulan bilgisayar uzmanı görüşleri dikkate alınmamıştır.*
- CD'de yer alan bilgilerin atılması konusundaki titizlik, mahkeme katibinin huzurunda dile getirilmemiştir.*
- Polisin katkıda bulunduğu e-postalar yargı denetimi dışındaydı ve ilgili taraflar arasında herhangi bir çelişki yoktu.*

- Mahkeme katibi huzurunda Microsoft tarafından sağlanan CD'de yer alan belge, destek ve dosyalarda yargılanan olaylarla ilgili herhangi bir e-posta bulunamamıştır.*
- Polis merkezinde sanığın fotoğrafla tanınmasını gerçekleştiren tanıklar, adliyede (örneğin soruşturma aşamasında veya sözlü yargılama aşamasında) ifade vermemişlerdir, bu nedenle ilk müdahalenin delil değeri yoktur.*





Bu proje Avrupa Birliđi tarafından
finanse edilmektedir.

Son olarak, Yüksek Mahkeme, Ildefonso Nazario ve Fructuoso Gonzalo arasında yapılan yazışmaların içeriđine ilişkin geçerli bir delil bulunmadıđı ve bu nedenle herhangi bir yolsuzluk suçunun olmadıđı sonucuna varmıřtır.

EK ÇALIřMA MATERYALLERİ VE KAYNAKLARI

- [ADLİ VE İDARİ YARGILAMALARDA ELEKTRONİK DELİLLER, Avrupa Konseyi e-kitap](#)
- [Dijital Delil Toplanması ve Analizine Yeni Yaklaşımlar, Ulusal Adalet Enstitüsü Dergisi \(ABD\), Sayı No. 280, Yayımlanma tarihi: Ocak 2019 \(New Approaches to Digital Evidence Acquisition and Analysis, National Institute of Justice Journal \(USA\), Issue No. 280, Published January 2019\)](#)
- <https://eur-lex.europa.eu/homepage.html>
- <https://www.echr.coe.int/Pages/home.aspx?p=home&c=>
- https://curia.europa.eu/jcms/jcms/j_6/
- Kişisel verilerin işlenmesi karşısında gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin 2016/679/AB sayılı Tüzük
- Yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair 2016/680 sayılı Direktif
- Avrupa Parlamentosu ve Konseyi'nin ceza davalarında elektronik deliller için Avrupa Üretim ve Muhafaza Emirlerine ilişkin Tüzük Teklifi





Bu proje Avrupa Birlięi tarafından
finanse edilmektedir.

EĞİTİM PLANI

Başlıca amaçlar ve hedefler aşağıdaki hususlara ilişkin fikirlerin açıklığa kavuşturulmasıdır:

- Dijital delilin avantajları/dezavantajları
- Dijital delilin özellikleri
- Dijital delile karşı temel haklar
- Dijital deliller hakim ve savcılara nasıl yardımcı olabilir?
- Görünüşün deęiřmesi: Kağıt üzerinde içerik/dijital bilgiler
- Tanımlar
- Adli davalarda ve idari davalarda temel kılavuz ilkeler
- Karşılıklı Adli Yardımlaşma-Karşılıklı Adli Yardımlaşma Talebinde nasıl bulunulur?
- Siber suçlarla ilgili uluslararası antlaşmalar ve İspanya mevzuatı

Pratik davalar aracılığıyla öğrenme

- Her davanın dikkatli bir şekilde okunması
- Bu örneklerin başlıca hususlarına ilişkin genel ve spontane tartışma
- Eğitici tarafından belirtilen fikirler veya sorulara ilişkin spesifik tartışma

Seminerin uzunluęu

2 gün:

- 1. Gün: Yazılı olarak sunulan konuların sözlü olarak açıklanması ve dijital delillerin deęerlendirilmesinin yasal dayanaklarının ayrıntılı bir şekilde açıklanması
- 2. Gün: AİHM içtihadına dayalı olarak pratik davalar ve dięer ölkelerde elde edilen deneyimler

Lojistik gereklilikler

Tartışmalara tam katılım sağlamak amacıyla, katılımcılar, her birinde en fazla 10 kiři olacak şekilde 4 gruba ayrılmalıdır. İki grup A davasını incelerken dięer iki grup B davasını inceleyecektir. Bu oturumların sonunda, dört grup bir araya gelecek ve kendi ulaştıkları sonuçlarla her iki davaya ilişkin genel deęerlendirmeye katkıda bulunacaktır.





Bu proje Avrupa Birliđi tarafından
finanse edilmektedir.

DEĞERLENDİRME FORMU

Dijital delillerin değ erlendirilmesi

Faaliyetin ne kadar ilginizi çekti ve sizin iş iniz ne kadar faydalı oldu? (1 hiç 10 çok yüksek anlamına gelmektedir).

<i>İlgi çekicilik</i>	1	2	3	4	5	6	7	8	9	10
<i>Fayda</i>	1	2	3	4	5	6	7	8	9	10

- Lütfen faaliyetin içeriđiyle ilgili olarak aşı ğ ıdaki ifadelerden hangisine katıldığ ınızı iş aretleyiniz:
- Faaliyet konuları, uygulamadan ziyade daha çok teorik veya doktrine yönelikti.
- Faaliyet konularına yönelik yaklaş ım teorikten ziyade daha çok uygulamaya yönelikti.
- Faaliyetin konusuna yönelik teorik ve uygulamaya yönelik yaklaş ımlar dođ ru bir şekilde birleřtirilmiř ti.
- Lütfen faaliyetin aşı ğ ıda belirtilen hususlarıyla ilgili memnuniyet düzeyinizi belirtiniz (1 hiç 10 çok yüksek anlamına gelmektedir).

<i>Belgelerin seğı imi</i>	1	2	3	4	5	6	7	8	9	10
<i>Eđ iticiler tarafından sunulan belgeler (nicelik)</i>	1	2	3	4	5	6	7	8	9	10
<i>Eđ iticiler tarafından sunulan belgeler (nitelik)</i>	1	2	3	4	5	6	7	8	9	10
<i>Faaliyetin uygulanmasında faaliyeti düzenleyenler ve eđ iticiler tarafından gösterilen ilgi</i>	1	2	3	4	5	6	7	8	9	10
<i>Katılımcıların faaliyete gösterdiđ i ilgi</i>	1	2	3	4	5	6	7	8	9	10
<i>Zaman dađ ılımı</i>	1	2	3	4	5	6	7	8	9	10





Bu proje Avrupa Birlięi tarafından
finanse edilmektedir.

Genel olarak organizasyon

1 2 3 4 5 6 7 8 9 10

➤ Faaliyetin süresiyle ilgili olarak aşağıdaki ifadelerden hangisine katıldığınızı işaretleyiniz:

☐ Çok uzundu, daha kısa olabilirdi.

☐ Süre uzatılmalıdır.

☐ Faaliyetin içerięi ve süresi iyi ayarlanmıştı.

➤ Bu konuyla ilgili faydalı sonuçlara ulaşıldı mı?

☐ Evet

☐ Hayır

➤ Sizce, faaliyeti düzenleyenler ve eğitimciler, ilgili konular hakkında deneyim ve görüş paylaşımını teşvik etti mi?

☐ Evet

☐ Hayır

➤ Faaliyetin konusu göz önünde bulundurulduğunda, sizce

☐ Eğitimcilerin mesleki arka planı uygun muydu?

☐ Farklı bakış açılarına katkıda bulunan diğer meslek gruplarından konuşmacı eksikliği var mıydı?

➤ Faaliyeti genel olarak değerlendirdiğinizde 1 ila 10 arasında kaç puan verirsiniz?:



