Avrupa Konseyi Budapeşte Sözleşmesi Kapsamında Saklama Talebi ve Türkiye Uygulamaları Çalıştay Raporu

EMNİYET GENEL MÜDÜRLÜĞÜ
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

İçindekiler

1. Giriş 3
2. Soru ve Senaryoların Tartışılması 6
2.1 Soru 1 - Acil Yardım 6
2.2 Soru 2 - Veri Kategorileri 7
2.3 Soru 3 - 7/24 Temas Noktasının Suç Soruşturması Kapsamı Dışında Bilgi Paylaşımına İzin Verilmesi 9
2.4 Soru 4 - Bilgi Paylaşımında Cezai Sorumluluk 10
2.5 Soru 5 - Bilgi Paylaşılmaması Durumunda Sorumluluk 11
2.6 Soru 6 - Türk Vatandaşları ve Yabancı Ülke Vatandaşları Hakkında Bilgi Paylaşımı 13
2.7 Soru 7 - Bildirmeme Yükümlülüğü 14
2.8 Soru 8 - Verileri Silmeme Yükümlülüğü 16
2.9 Soru 9 - Tüzel Kişilerin Yükümlülükleri 17
2.10 Soru 10 - İşbirliğinden Kaçınma 18
2.11 Soru 11 - Şüpheli Para Transferlerinin Durdurulması 19
2.12 Soru 12 - Kolluk Kuvvetlerinin Şüpheli Banka Hesaplarını Resen Dondurması 22
2.13 Soru 13 - Yabancı Mağdurlarun Resmi Şikayetlerinin Aranması 22
2.14 Soru 14 - Saklama Süresi Dolan Verilerin Kullanımı 23
2.15 Soru 15 - Trafik Verilerinin Gerçek Zamanlı Toplanması ve Kısmen Açıklanması 25
2.16 Soru 16 - İçerik Verileri İçin İletişimin Denetlenmesi Tedbiri 27
2.17 Soru 17 - Kendiliğinden Bilgi Verme 28
2.18 Soru 18 - İnternet Servis Sağlayıcıları ile Daha Etkin İşbirliği 29
3 Sonuç 32
4 Katılımcı Listesi 33

Feragat Beyanı:

Bu teknik rapor, Avrupa Konseyi'nin, etkinliği kısmen fonlayan iPROCEEDS projesinin ve Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesine taraf üye ülkelerin resmi pozisyonlarını yansıtmamaktadır.

1. Giriş

Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ("Sözleşme"), 2001 yılında Macaristan'ın Budapeşte kentinde imzalanarak yürürlüğe girmiştir. İnternet ortamında ve bilgisayar sistemlerine yönelik işlenen suçlar hakkında düzenlenen ilk uluslararası metin olma özelliğini taşıyan Sözleşme'nin temel amaçları; siber suçlara ilişkin suç fiillerinin ceza kanunlarında tanımlanmasında ülkeler arasında yeknesaklığın sağlanması, adli birimlerin ülke dışındaki dijital delillere erişilebilirliğine yönelik tedbirlerin süratle alınması ile siber suçlarla mücadelede uluslararası işbirliğinin ve teknik bilgi paylaşımının daha etkin bir düzeye getirilmesidir.

Sözleşme'ye, Avrupa Konseyi üyesi olmayan Amerika ve Japonya gibi ülkelerle birlikte 60'tan fazla üye ülke taraftır. Ayrıca anlaşmayı imzalamamış bazı ülkeler de, Sözleşme'deki suç tanımları ve diğer güvenlik tedbirlerinden ilham alarak yasal altyapılarında değişikliğe gitmişlerdir.. Türkiye, Sözleşme'yi 10 Kasım 2010 tarihinde imzalamış, 22 Nisan 2014 tarihinde Türkiye Büyük Millet Meclisi Genel Kurulunda görüştükten sonra onaylamıştır. 2 Mayıs 2014 tarihinde 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin Onaylanmasının Uygun Bulunduğuna Dair Kanun'un Resmi Gazete'de yayımlanması ile Sözleşme yürürlüğe girmiştir.

Geleneksel suç soruşturmalarına konu olan fiziksel delillerin aksine, dijital verilerin erişilebilirliği daha kırılgan bir yapıya sahiptir ve hızlı bir biçimde bu delilleri korumaya yönelik yasal tedbirler uygulanmadığında suç soruşturmaları sekteye uğrayabilir. Sözleşme, genellikle aylar süren adli istinabe süreci sonunda talebe konu olan dijital delillerin teminini garanti altına almak için, 29. maddesiyle "saklama talebi" kavramını oluşturmuştur. Sözleşme'nin 35. maddesine dayanarak kurulan ulusal temas noktaları, saklama taleplerini ilgili servis sağlayıcılara bildirir ve servis sağlayıcılar da adli istinabe talebi kendilerine ulaştığında bahse konu dijital delilleri talep eden ülkenin adli makamlarına teslim eder. Bu kapsamda, Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, Türkiye adına 7/24 Ulusal Temas Noktası görevini yürütmektedir. Saklama talepleri ve acil durumlarda yapılan bilgi taleplerine ek olarak talepte bulunan ülkelere, suç soruşturmasına ilişkin konularda teknik ve yasal danışmanlık hizmeti de sağlanmaktadır.

Ulusal Temas Noktası, uluslararası polis işbirliği kanallarından biri olup niteliği gereği sadece acil durumlarda kullanılmaktadır. Kolluk kuvvetleri tarafından Interpol ve Europol kanalları yoğun olarak kullanılmakta ve ayrıca yabancı polis irtibat görevlileri kanalıyla da bilgi ve tecrübe alışverişi yüz yüze yapılmaktadır. Mevcut haliyle Ulusal Temas Noktası aracılığıyla yürütülen hizmetler, toplam uluslararası polis işbirliğinin küçük bir yüzdesini oluşturmaktadır. Ülkemize gelen saklama taleplerinin sayısının az olmasının ana sebebi olarak yabancılar tarafından kullanılan Türkiye merkezli servis sağlayıcısının sayısının ve doğal olarak da yabancı mağdur

sayısının nispeten düşük olması gösterilebilir. Ülkemizden gönderilen saklama taleplerinin sayısının az olmasının ise, ülke içerisinde Ulusal Temas Noktası'nın yürüttüğü hizmetlere ilişkin bilgi eksikliğinden kaynaklandığı değerlendirilmektedir. Diğer ülkelerde de benzer sıkıntıları gözlemleyen Avrupa Konseyi Siber Suç Komitesi, Ulusal Temas Noktalarının yetkilerinin ülke içerisindeki diğer paydaşlara daha etkin bir biçimde tanıtılmasına ilişkin tavsiye kararı almıştır.[1]

Türkiye'de Sözleşme'nin maddi ceza hukukunu ilgilendiren hükümlerine ilişkin uyumlaştırma çalışmaları yapılmıştır. Ancak saklama talepleri ve hızlandırılmış uluslararası bilgi paylaşımı başta olmak üzere, Ulusal Temas Noktası'nın görev alanına giren konularda yasal bir düzenleme yapılmamıştır. Şu ana kadar kanunla kendisine verilen yetkiyi kullanan Ulusal Temas Noktası, iç hukuk sistemiyle çelişmeyecek bir şekilde saklama taleplerinin ve diğer acil taleplerin gereğini yapmıştır. Ancak detaylı yasal düzenlemelerin olmaması ve servis sağlayıcıların tabi olduğu mevzuat ile Sözleşme'nin getirdiği yükümlülükler bakımından farklılıklar olabilmesi, uygulamada zaman zaman tereddütler yaşanmasına yol açmaktadır.

Gerek Ulusal Temas Noktası'nın yurt içindeki paydaşlara tanıtımını yapmak gerekse ilerleyen zamanlarda yapılacak Sözleşme'nin Türk hukukuna daha kapsamlı uyumlaştırılma çalışmalarına fikri kaynak yaratmak adına; hakimler, savcılar, adalet bakanlığı yetkilileri, erişim ve yer sağlayıcıları ile akademisyenler, İstanbul'da 15-16 Nisan 2019 tarihlerinde düzenlenen "Budapeşte Sözleşmesi Kapsamında Saklama Talebi ve Türkiye Uygulamaları" isimli çalıştaya davet edilmişlerdir. Katılımcılara etkinlikten önce, Ulusal Temas Noktası yetkililerinin derin tecrübeleri ışığında hazırlanan ve siber suçlarla mücadelede dünyada tartışma konusu olan güncel gelişmeleri de yansıtan 18 adet soru ve senaryo ile Sözleşme'nin açıklayıcı notlarının gayrıresmî Türkçe çevirisi e-posta yoluyla gönderilmiştir. Avrupa Konseyi IPROCEEDS projesi[2] tarafından da kısmen fonlanan çalıştayın ilk gününde Fransa, Letonya ve Romanya Ulusal Temas Noktalarının sunumları gerçekleştirilmiştir. Yabancı Ulusal Temas Noktalarına gönderilen sorular ve senaryolar ise daha genel nitelikte olup sadece Türk hukukunu ilgilendiren kısımlar kendilerine iletilmemiştir. Etkinliğin geri kalan bölümünde ise katılımcılar 5 grup halinde moderatör tarafından kendilerine verilen süre çerçevesinde tartışma gerçekleştirmişlerdir. Daha sonra grupların görüşleri ve karşıt görüşleri ifade edilmiştir. Elektronik ortamda kayıt altına alınan bu konuşmalar, okuyucuyu uzun bir metinle sıkmamak ve tüm fikirleri yansıtabilmek arasında ince bir denge gözetilmek suretiyle anonimleştirilerek derlenmiştir. Yabancı Ulusal Temas Noktalarının cevapları da uygun yerlerde özetlenerek ilgili cevapların altına eklenmiştir. Belirtmek gerekir ki, Budapeşte Sözleşmesi ve açıklayıcı notları ile katılımcıların hukuki yorumları arasında çelişkiler olması durumunda, Budapeşte Sözleşmesi ve açıklayıcı notları esas alınmalıdır.

1 Tavsiye kararı 5, T-CY değerlendirme raporu: Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesindeki karşılıklı adli yardım maddeleri, 2014, sf. 125 https://rm.coe.int/t-cy-2017-18-opinion-article29-/168076cf95

2 https://www.coe.int/en/web/cybercrime/iproceeds

Ulusal Temas Noktası yetkilileri, bu çalıştay için NATO'nun siber çatışma ve siber savaş hallerinde uygulanabilecek olası uluslararası hukuk kurallarını ele aldığı Talinn kitapçığından ilham almıştır. Çalıştay raporunun İngilizce ve Türkçe dillerinde çevrimiçi açık kaynaklarda yayınlanması ile hem diğer ülkelerin Ulusal Temas Noktalarının benzer çalışmalar yapmasına hem de yurtiçindeki akademik tartışmalara ve olası yasal düzenlemelere ilham verme amacı hedeflenmiştir.

Ulusal Temas Noktası yetkilileri olarak, çalıştayın gerçekleştirilmesinde maddi ve manevi desteğini esirgemeyen Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanı Sayın Erdal ÇETİNKAYA ile Avrupa Konseyi IPROCEEDS projesi yöneticilerine ve eşsiz tecrübelerine dayanan değerli fikirleriyle bu raporun ortaya çıkmasında büyük katkıları olan değerli katılımcılarımıza teşekkür ediyoruz.

2. Soru ve Senaryoların Tartışılması

2.1 Soru 1 - Acil Yardım

Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin ("Sözleşme") 35. maddesinde tanımlanan "Acil Yardım (Immediate Assistance)" kavramının kapsamını Türk hukuk sistemi ve evrensel hukuk ilkeleri bağlamında tartışınız.

- **Sadece insan hayatına veya kişilerin vücut bütünlüğüne yakın tehlike olan durumlar mı bu kapsam içinde değerlendirilmeli?**
- **Mal varlığına veya kritik dijital verilere yönelik durumlar da bu kapsama dahil edilmeli mi? Lütfen örnek olaylarla uzman görüşünüzü açıklayınız.**

Moderatör, uluslararası polis işbirliği kapsamında ülke kolluk kuvvetleri arasındaki bilgi alışverişi için Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin (Bundan sonra "Sözleşme" olarak geçecektir) 7/24 Ulusal Temas Noktası da dahil birçok resmi ve gayrıresmî iletişim kanallarının olduğu ve ülkeler tarafından en yoğun olarak Interpol'ün iletişim sisteminin kullanıldığı hakkında genel bir bilgilendirme yaparak oturumu açmıştır. Katılımcılar, insan hayatına veya kişilerin vücut bütünlüğüne yakın tehlike olması durumunun "acil yardım" kapsamında değerlendirilmesinde ve Türk hukukunda kendisine yer bulamayan bu kavramın açıkça düzenlenmesi gerektiğine dair görüş birliğine varmıştır. Ancak, bunun dışında kalan diğer durumlar için değişik hukuki yorumlar ortaya çıkmıştır. Sözleşme metnine ve açıklayıcı notlarına atıf yapan bazı katılımcılar, Sözleşme'nin "acil yardım" kavramının, usül hükümlerine ilişkin bir kavram olduğundan bahisle dijital delillerin bulunduğu her türlü suç türü için uygulanabileceğini iddia etmiştir. Kimi katılımcılar ise böylesi geniş bir yorumun, Türk Ceza Kanunu'nun 135 ve 136. maddesindeki kişisel verilere ilişkin maddelere aykırılık yaratabileceği uyarısında bulunmuşlardır. Bu kapsamda, Ulusal Temas Noktası'na ulaşan her talebin kişisel haklar bağlamında süzgeçten geçirilerek, bireysel menfaatlerin kamusal menfaatlerden baskın olduğu durumlarda, bu yola tenezzül edilmemesi gerektiğini vurgulamışlardır. Ayrıca birçok katılımcı, Türk hukukundaki "telafisi güç veya imkansız zararlar doğması" kavramına da atıfta bulunarak, dijital verilerin erişilebilirliğinin kolaylıkla ortadan kalkabileceği ve bu sebeple acil yardım kapsamının mal varlığına karşı suçlar, kritik altyapılara yönelik bilişim suçları ve çevrimiçi çocuk istismarı gibi diğer suçları da içine alacak şekilde genişletilebileceğini ileri sürmüşlerdir. Son olarak bir katılımcı, "acil yardım" kavramının tamamıyla yanlış yorumlandığı ve aslında Sözleşme'de kast

edilenin "anında yardım" olduğu hususundaki yorumlarını iletmiştir. Talebe konu olan suçun niteliğinden bağımsız olarak aslında, Ulusal Temas Noktası tarafından talepte bulunan ülkeye yapılan hızlı ve etkili yardımın tanımlandığı iddia edilmiştir.

Letonya Ulusal Temas Noktası yetkilisi, ülkesinde terör saldırısı tehditlerinin ve kişilerin can güvenliğinin tehlikede olduğu durumların acil durum olarak nitelendirildiğini belirtmiştir.

ÖNEMLİ NOT: Ulusal Temas Noktası'na diğer ülkelerden gönderilen her talep, ülkemizde adli soruşturma açılmasını gerektirmeyebilir. Bu sebeple aşağıdaki soruları cevaplarken hem Cumhuriyet Savcısı'nın soruşturma açtığı hem de açmadığı/açamayacağı seçenekleri değerlendirerek cevaplayınız.

2.2 Soru 2 - Veri Kategorileri

A ülkesinin Ulusal Temas Noktası'nın ilettiği acil yardım talebini, ülkemiz Temas Noktası gecikmeksizin ilgili internet servis sağlayıcısına iletir. Talep, belirli bir internet sitesindeki belirli bir kullanıcının abone kimlik bilgilerini (subscriber information), bu kullanıcının internette erişim sağladığı tüm IP adreslerini (traffic data) ve bu kullanıcının bir sitede belli bir zaman diliminde ürettiği tüm içerikleri (content data) kapsamaktadır. Abone kimlik bilgilerinin iç hukukumuzda açık bir tanımı yapılmadığını göz önünde bulundurarak aşağıdaki kavramsal tartışmalara ve olası senaryolara ilişkin uzman görüşünüzü açıklayınız.

- **Sizce abone kimlik bilgileri ne çeşit verileri içermelidir ve hangi yasal düzenlemeyle sınırları belirlenmelidir?**
- **Bazı internet servis sağlayıcıları, bir kullanıcının hesabına erişen son 50/100 IP adreslerini (son erişim IP adresleri) de abone kimlik bilgisi olarak tanımlamaktadır. Sizce benzer bir uygulama Türk hukuk sistemine göre yapılabilir mi?**
- **İçerik verisine ilişkin iç hukukumuzda herhangi bir atıf yapılmamıştır. Sizce bu kanuni boşluğun doldurulması gerekir mi?**

Lütfen somut örneklerle yukarıdaki sınıflandırmanın yasal gerekliliğini veya veri

tanımlarının Sözleşme'ye tam uyumlu hale getirilmesine lüzum olup olmadığını tartışınız.

Moderatör, gelen sorular üzerine, son erişim IP adresleri (last login IPs) kavramını açıklayarak oturumu başlatmıştır. Web siteleri, kendi kullanıcılarının siteye erişim yaptıkları IP adreslerine ilişkin bilgiyi muhafaza etmektedir. Yabancı internet servis sağlayıcıları, bir kullanıcının abone kimlik bilgileri talep edildiğinde, sayısı genelde 10 ile 100 arasında değişen IP adresi ve erişim zaman bilgisini kolluk kuvvetlerine iletmektedir. Bu bilgilerle ilgili kullanıcıya ilişkin, sadece belli bir zaman diliminde belirli bir web sitesine eriştiğinden başka bir kişisel bilgiye ulaşılamamaktadır. Bu uygulamanın arkasındaki mantık, tek bir IP adresi ve erişim zamanı bilgisi temin edildiğine, VPN (Virtual Private Network) kullanan veya internet servis sağlayıcı tarafından NAT IP (Network Address Translation) atanan bir kullanıcının tespitinin mümkün olmamasıdır. Birden fazla bağlantı bilgisi, ilgili kullanıcının gerçek kimliğine ulaşılması ve doğrulanması açısından büyük önem taşımaktadır.

Birçok katılımcının Sözleşme'nin 18. maddesindeki abone kimlik bilgisinin ayrıntılı tanımını işaret etmesine rağmen, abone kimlik bilgisinin kapsamı hakkında tam bir görüş birliğine varılamamıştır. Ancak tüm katılımcılar, bu eksikliğin yasal düzenleme yapılarak giderilmesi hususunda hemfikir olmuşlardır. İlgili yasal değişiklik için, katılımcıların çoğu 5651 sayılı 'İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"u veya bu kanunda geçen ilgili tanımı açıklayacak bir yönetmeliği işaret ederken bir katılımcı da, 5809 sayılı "Elektronik Haberleşme Kanunu"ndaki "abone kimlik ve iletişim bilgileri" tanımının genişletilebileceği yorumunu getirmiştir. Ayrıca bir katılımcı, Sözleşme'nin açıkça abone kimlik bilgisinin trafik bilgisinden farklı olduğunu belirttiğini vurgulamış ve usul hukuku yönünden, abone kimlik bilgisi için "üretim emri" ile trafik bilgisi için "koruma emri" kavramlarının getirildiğinin altını çizmiştir. Sözleşme'ye taraf olan üye ülkelerle işbirliğinde uygulamada sorunlar yaşanmaması adına, 5651 sayılı kanundaki trafik bilgisi tanımından abone kimlik bilgisi ifadesinin çıkarılması gerektiği savunulmuştur. Yukarıda bahsi geçen son erişim IP adreslerine ilişkin ise kullanıcının özel hayatının gizliliğini ihlal edecek biçimde internet gezinme geçmişini ifşa ederek kullanıcı profili oluşturulmasına müsaade etmediği müddetçe, olumlu değerlendirilebileceğine yönelik görüşler hasıl olmuştur.

İçerik verisinin kapsamına ilişkin yasal düzenleme eksikliğinde birleşen katılımcılar, bunun hangi yasa kapsamında olabileceğine ilişkin farklı önerilerde bulunmuştur. 5651 sayılı 'İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", 5809 sayılı "Elektronik Haberleşme Kanunu" veya 6698 sayılı "Kişisel Verilerin Korunması Kanunu" gibi ilgili mevzuatın bir veya birkaçının güncellenip terim birliğinin oluşturularak uygulamada yaşanabilecek tereddütlerin ve doğabilecek mağduriyetlerin

önlenmesi vurgulanmıştır. Bazı katılımcılar, 5651 sayılı kanun erişim sağlayıcılarının trafik verilerini saklama yükümlülüklerine ilişkin açık kurallar getirirken, içerik sağlayıcılarının yasal sorumluluklarına ve içerik verilerine ilişkin büyük bir boşluğun olduğunu belirtmişlerdir. Soruşturma ve kovuşturma aşamasında dijital delillerin erişilebilirliğinin sağlanması ile içerik sağlayıcılarının hukuki ve cezai sorumluluklarının nesnel kriterlerle tespit edilebilmesi adına ilgili yasal altyapının oluşturulması gerekliliğini işaret etmişlerdir. Ayrıca bir katılımcı, içerik verisi kavramının Türk hukukundaki yansımalarına ilişkin ilginç bir bakış açısı getirmiştir. 5651 sayılı Kanun'un internet ortamında sunulan içerikleri kapsadığını, 5809 sayılı Kanun'la ise iki bilgisayar sisteminin arasında gerçekleşen ancak internette yayınlanmayan içerik verisinin düzenlendiğini ve son olarak Ceza Muhakemesi 135. maddesinin iki kişi arasındaki iletişime ilişkin içerik verilerini konu aldığını belirterek içerik verisi kavramına ilişkin teorideki ve uygulamadaki dağınıklığı gözler önüne sermiştir.

2.3 Soru 3 - 7/24 Temas Noktasının Suç Soruşturması Kapsamı Dışında Bilgi Paylaşımına İzin Verilmesi

Polis Vazife ve Salahiyetleri Kanunu Ek Madde 6'da 2017 yılında yapılan bir değişiklikle "Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet Başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri, kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir." hükmü getirilmiştir.

- **Türkiye'de soruşturmaya konu olamayacak bir bilgi talebi olması durumunda, Ulusal Temas Noktası'nın yukarıdaki maddeye dayanarak doğrudan bilgi paylaşımı yapması mümkün müdür?**
- **Mümkün değilse Ulusal Temas Noktası'na bu yetkiyi kazandırmak adına; hangi yasal düzenlemeler yapılmalıdır?**

Katılımcıların büyük çoğunluğu, PVSK ek madde 6'nın sadece Cumhuriyet Savcılığının tespiti amacıyla kolluk tarafından abone kimlik bilgisi sorgulanmasına cevaz verdiğini belirterek Cumhuriyet Savcısı'nın dahil edilmediği senaryolarda bu yetkinin kullanılamayacağını ifade

etmişlerdir. Bazı katılımcılar, Ulusal Temas Noktası'na suç soruşturması dışı bilgi paylaşımı yetkisi verilmesinin gerekliliğinin etraflıca tartışılmasını işaret ederken bazı katılımcılar ise yapılacak kanuni düzenlemeyle veya ülkeler arası antlaşmalarla sınırlı biçimde bilgi paylaşımı yetkisi kazandırılabileceğini belirtmişlerdir. Bahse konu maddenin mevcut Türk hukuk sistemine uygunluğunu sorgulayan katılımcılar bulunması üzerine bir katılımcı, kolluğa neden bu yetkinin verildiğini detaylıca açıklamıştır. Özellikle ABD'de ki National Centre for Missing and Exploited Children (NCMEC) isimli sivil toplum kuruluşundan yine ABD'de mukim Facebook, Google ve Twitter gibi internet servis sağlayıcılarının platformlarına çevrimiçi çocuk istismarı yükleyen kullanıcılara ait raporlar öncelikle Siber Suçlarla Mücadele Daire Başkanlığına ve daha sonra ilgili illerin Cumhuriyet Savcılığına gönderilmektedir. Kolluğa doğrudan abone kimlik bilgisi sorgulaması yetkisi verilmeden önce, raporların büyük çoğunluğu belli illerde yoğunlaşmıştır. İlgili ilin Cumhuriyet Savcılığı tarafından yer tespiti yapıldığında ise birçok kullanıcının aslında başka illerde ikamet ettiği ortaya çıkmıştır. Bu ve benzeri sebeplerle, kimi zaman bazı şüphelilere ulaşmak iki yıla kadar zaman almıştır. Suçla mücadelede dijital delillere daha hızlı erişmek ve delillerin etkin bir biçimde muhafazasını sağlamak adına kanun koyucu, kolluğun doğrudan abone kimlik bilgisini sorgulama yetkisini getirmiş ve yukarıda ayrıntılandırılan sürecin dikkate değer biçimde kısalmasını sağlamıştır.

2.4 Soru 4 - Bilgi Paylaşımında Cezai Sorumluluk

Türkiye Cumhuriyeti Anayasası Madde 90'a göre, "Usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir. Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır." Bu maddeye dayanarak iç hukukta, açıkça belirtilen bir zorunluluk olmamasına rağmen internet servis sağlayıcısı, gerekli bilgiyi Ulusal Temas Noktası'na sağlar. Ancak daha sonra, Cumhuriyet Savcısı tarafından Ulusal Temas Noktası ve internet servis sağlayıcısı hakkında, hukuka aykırı işlem tesis ettikleri gerekçesiyle ceza soruşturması açılır.

- **Yukarıdaki olayda, Temas Noktası ve internet servis sağlayıcısının Türk Ceza Kanunu'na göre cezai sorumluluğu var mıdır?**

- **Cevabınız evet ise cezai sorumluluğun kaynağını ve sorumluluğu kaldırmak**

için hangi yasal metinlerde değişiklikler yapılması gerektiğini etraflıca açıklayınız. Eğer cezai sorumluluk olmadığını düşünüyorsanız, yapılan işlemin neden hukuka uygun olduğunu izah ediniz.

Birkaç katılımcının tereddütlerine karşın, Sözleşme'nin tartışmasız biçimde temel insan haklarına ve özgürlüklerine ilişkin olduğu ve bu sebeple, Türk hukuk sisteminde kanunların üstünde bağlayıcılığı olan bir metin olduğu yönünde çoğunluk görüşü oluşmuştur. Sözleşme'nin arama, el koyma ve iletişimin gerçek zamanlı denetlenmesi gibi koruma tedbirleriyle, özel hayatın gizliliğini ve ifade hürriyetini yakından etkilemesi, destekleyici bir argüman olarak sunulmuştur. Dolayısıyla iç hukukta açıkça tanımlanmış bir yetki ve sorumluluk bulunmasa bile Sözleşme'nin 18. maddesine dayanarak Ulusal Temas Noktası'na abone kimlik bilgisi veren internet servis sağlayıcılarının cezai sorumluluğu olmayacağı ifade edilmiştir. Bu durumda, Türk Ceza Kanunu'nun 24. maddesinde belirtilen "kanun hükmünü yerine getirme" hukuka uygunluk nedeninin gerçekleşeceği vurgulanmıştır. Ulusal Temas Noktası'nın diğer ülke Temas Noktalarıyla bilgi paylaşımı yapması hususunda ise Türkiye'de suç soruşturmasına konu olabilecek hallerde aynı hukuka uygunluk nedeninin oluşacağında fikir birliğine varılmıştır. Her ne kadar Sözleşme, uluslararası işbirliği için çifte suçluluk şartı aramasa dahi Türkiye'de suç soruşturması açıl(a) mayan bir durumda, Ulusal Temas Noktası'nın diğer ülke Temas Noktalarıyla bilgi paylaşımı yapabilmesi için yasal düzenleme gerektiği yönünde yorumlar gelmiştir. Bir katılımcı ise 6698 sayılı Kanun'un 8. maddesine göre kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağını ve bu kuralın istisnalarının da aynı maddede sayıldığını belirtmiştir. Bu kapsamda, Ulusal Temas Noktası ve internet servis sağlayıcısının hukuka uygun olmayan bilgi paylaşımı gerçekleştirdikleri için cezai sorumluluklarının doğacağı ve bunu engellemek için Ulusal Temas Noktası tarafından yapılacak uluslararası bilgi paylaşımına ilişkin yasal düzenleme yapılması gerekliliğinin altını çizmiştir.

2.5 Soru 5 – Bilgi Paylaşılmaması Durumunda Sorumluluk

İnternet servis sağlayıcısı, iç hukukta açıkça öngörülmüş bir kural olmadığından bahisle, Temas Noktası ile doğrudan bilgi paylaşımı yapmaktan çekinir ve savcılık talimatı veya mahkeme kararı talep eder. Fakat yargı makamları, ilgili isteğin diplomatik kanallardan adli istinabe talebiyle gelmesi halinde gereğinin yapılacağını ifade eder. Bu esnada, bahse konu suç A ülkesinde meydana gelir ve sonucunda maddi hasar, zarar veya

kayıp meydana gelir.

- **Ulusal ve uluslararası hukuk açısından herhangi bir şahıs veya kurumun A ülkesinde meydana gelen suç için yasal sorumluluğu iddia edilebilir mi?**

- **Yukarıdaki olayda, yargı makamlarının yetkisizlik kararı vererek bilgi talebini değerlendirme dışı bırakmaları mümkün müdür?**

Bu sorunun cevabında da, Sözleşme'nin Türk hukuk sistemindeki yerine ilişkin katılımcılar arasındaki görüş ayrılıkları su yüzüne çıkmıştır. Bazı katılımcılar, internet servis sağlayıcısının, kanun hükmünü yerine getirmediği için cezai sorumluluğu doğacağını ileri sürmüşlerdir. A ülkesinde meydana gelen bir zarardan bağımsız olarak, hem servis sağlayıcının hem Cumhuriyet Savcısı'nın görevi ihmal ve/veya görevi kötüye kullanma suçlarından işlem görebileceği işaret edilmiştir. Bir katılımcı ise Birleşmiş Milletler Uluslararası Hukuk Komisyonu'nun 2001 yılı tarihli "Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni"ne atıfta bulunarak açık ve sistematik olarak uluslararası bir yükümlülüğün yerine getirilmesinin ağır ihlal kavramıyla tanımlandığı ve bu çerçevede devletlerin de sorumlu tutulabileceği yorumunu yapmıştır. Bazı katılımcılar ise Sözleşme'de yer verilen yükümlülüklerin iç hukukta yasal düzenlemelerle desteklenmedikçe ilgili kişi ve kurumlara cezai sorumluluk yüklenemeyeceğini belirtmişlerdir. Bir katılımcı da, kanunla açıkça aksi öngörülmediği için Türk vatandaşlarına uygulanan kuralların ve prosedürlerin Ulusal Temas Noktası'na gelen talepler için de bağlayıcı olduğunu ifade etmiştir.

Yargı makamlarının, yetkisizlik kararı vererek Ulusal Temas Noktası'na gelen bir talebe yasal yollarla karşılık verilmesinin, imkansız hale gelme ihtimalinin olduğunda fikir birliği oluşmuştur. Bir katılımcı, Türk hukuk sistemine göre yetkili mahkemede dava açılacağı ve bu sebeple yetki tayininin önemini hatırlatmıştır. Aynı katılımcı, uygulamadaki olası yetki sorunlarını çözmek adına, Ulusal Temas Noktası'na gelen talepleri değerlendirmek için tüm Türkiye'de yetkili olan bir yargı makamının oluşturulmasının en ideal çözüm yöntemi olduğuna ilişkin değerlendirmelerini de iletmiştir.

Letonya Ulusal Temas Noktası yetkilisi, böyle bir durumda "İdari İhlalleri Kanunu" 175. maddesinin 2. fıkrasındaki "Denetleme veya Yerel Yönetim Kurumları Görevlilerinin Yasal İsteklerine Uymama" suçunun oluşacağını ve ilgili internet servis sağlayıcısının yasal sorumluluğunun doğacağını ifade etmiştir.

2.6 Soru 6 - Türk Vatandaşları ve Yabancı Ülke Vatandaşları Hakkında Bilgi Paylaşımı

Bu defa yargı makamları, internet servis sağlayıcısının talep ettiği emri verir. Söz konusu şüpheli kişi, ülkemizde yaşamakta olan yabancı uyruklu bir şahıstır. Yabancı uyruklu bir şahsın bilgileri başka bir ülke makamları ile paylaşılabilir mi?

- **Eğer bu soruya cevabınız olumlu ise bu paylaşımın sınırları nedir?**
- **Şüphelinin, Türkiye Cumhuriyeti vatandaşı olması durumunda, takip edilmesi gereken kurallar ve prosedürler farklılık gösterir mi?**

Lütfen diğer Ulusal Temas Noktalarıyla bilgi paylaşımında, talebe konu olan verinin çeşidine göre (abone kimlik-trafik-içerik) usul ve esasların belirlenmesi hakkında görüş ve önerilerinizi de paylaşınız.

Katılımcıların tamamı, Türk Ceza Kanunu'nun 8. maddesindeki mülkilik ilkesi gereği, Türkiye'deki yabancı ülke vatandaşlarına ve Türk vatandaşlarına ilişkin bilgilerin paylaşımında bir farklılık olamayacağını ifade etmiştirler. Bazı katılımcılar, istisnai durumlar olan, diplomatik dokunulmazlık gibi özel statü hallerini ve Anayasa'nın 16. maddesindeki "Temel hak ve hürriyetler, yabancılar için, milletlerarası hukuka uygun olarak kanunla sınırlanabilir." hükmüne ilişkin olası uygulamaları işaret etmişlerdir. Ancak Ulusal Temas Noktası'nın uluslararası bilgi paylaşımı yapması noktasında, yine iç hukuktaki yasal altyapı eksikliğine vurgu yapılmıştır. Ayrıca katılımcılar, talep edilen veri tipine göre bilgi paylaşımına ilişkin de yasal bir ayrıma gidilmesi gerektiğinde fikir birliğine varmışlardır.

Fransa ve Letonya Ulusal Temas Noktası yetkilileri, yabancı kişilerin bilgilerinin diğer Temas Noktalarıyla paylaşılmasına ilişkin özel bir düzenleme getirilmediğini belirtmişlerdir. Ayrıca yetkililer, ülkelerindeki uluslararası polis işbirliği çerçevesinde bilgi paylaşımına dair de bilgi vermişlerdir. Fransa Ulusal Temas Noktası yetkilisi, Fransa içinde soruşturma açılmasına gerek duyulmayan olaylarda, bilgi talep eden ülkeyle daha geniş kapsamlı işbirliği yapılabileceğini ifade etmiştir. Letonya Ulusal Temas Noktası yetkilisi ise, Letonya Anayasası'nın hükümlerinin, devlet egemenliği kavramlarının ve yerel soruşturmalara engel oluşturmamanın diğer ülkelerle yapılan bilgi paylaşımının doğal sınırlarını çizdiğini eklemiştir.

2.7 Soru 7 - Bildirmeme Yükümlülüğü

A ülkesi, kendi ülkesinde yaşayan bir çocuğun, çevrimiçi ayartılması (online grooming) olayı ile ilgili olarak Ulusal Temas Noktası'na bir veri saklama talebi gönderir. Temas Noktası, internet servis sağlayıcısından şüpheli şahsı, bu işlem hakkında bilgilendirmemesini talep eder. Şirket, şeffaflık politikası gereği ve iç hukukta bu gibi bir durumda bilgilendirmeme yükümlülüğü açıkça düzenlenmediği için, ilgili kişiyi saklama talebi hakkında bilgilendirir. A ülkesindeki suç şüphesinden haberdar olan kişi, kullandığı elektronik cihazlardaki tüm dijital materyalleri geri döndürülemeyecek bir şekilde siler. A ülkesinden adli istinabe talebi ulaşıp kişinin bilgisayar ve cep telefonu incelendiğinde bu kişinin, yurtdışında yaşayan çocukları, internet ortamında ayartmaya çalıştığına dair herhangi bir emareye ulaşılamaz.

- **Bu olayda, internet servis sağlayıcısının hukuki, idari ve cezai sorumluluğu var mıdır?**
- **Cevabınız olumlu ise ne tür bir müeyyide uygulanabilir?**
- **Cevabınız olumsuz ise benzer olaylarda, internet servis sağlayıcısına bilgilendirmeme yükümlülüğü getirmek adına hangi düzenlemeler yapılabilir?**

Katılımcılar, Türkiye'de suç soruşturmasına konu olabilecek bir bilgi talebi olması durumunda, Ulusal Temas Noktası'nın aksi yöndeki talimatına rağmen şüpheli şahsı bilgilendiren internet servis sağlayıcısının cezai sorumluluğu olacağını belirtmişlerdir. Türk Ceza Kanunu 285. madde 2. fıkrası olan "Soruşturma evresinde alınan ve soruşturmanın tarafı olan kişilere karşı gizli tutulması gereken kararların ve bunların gereği olarak yapılan işlemlerin gizliliğini ihlal eden kişi, bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılır." hükmüne atıfta bulunulmuştur. Türk Ceza Kanunu, tüzel kişilere ilişkin cezai sorumluluk öngörmediği için internet servis sağlayıcısının ilgili biriminde çalışan kişilerin, bu madde kapsamında cezalandırılabileceğini değerlendirmiştir. Bazı katılımcılar, bu maddenin ortaya çıkabilecek vahim sonuçlar karşısında yetersiz bir yaptırım olacağından bahisle, internet servis sağlayıcılarının suç soruşturmalarına ilişkin bilgilendirmeme yükümlülüğünün bağımsız bir suç tipi olarak daha ağır bir cezai müeyyideye tabii tutulmasının uygun olacağı yönünde görüş bildirmişlerdir. Böyle bir durumda, idari para cezalarının kurumsal açıdan daha caydırıcı olacağı yönünde yorumlar gelmiştir. 6698 sayılı Kanun'un 12. maddesindeki veri sorumlusunun muhafaza yükümlülüğünün ihlali ile 5651 sayılı Kanun'un yer sağlayıcı ve erişim sağlayıcının saklama yükümlülüğünün ihlali bağlamında yüklü idari para cezaları verilebileceği değerlendirilmiştir. Katılımcılar,

internet servis sağlayıcısının hukuki sorumluluğunun belirlenmesinde ise örnek olaydaki maddi ve manevi zararın tespit edilmesi ile bu zararın emre aykırı bilgilendirmeme yükümlülüğüne bağlanmasındaki zorluklara dikkat çekmiş ve net bir yorum yapmaktan kaçınmışlardır.

Türkiye'de suç soruşturmasının açıl(a)madığı durumlarda ise eğer şartları oluşmuşsa internet servis sağlayıcısının, görevi ihmal ve görevi kötüye kullanma gibi Türk Ceza Kanunu'ndaki genel hükümlere göre cezai sorumluluğunun olabileceği belirtilmiştir. Bazı katılımcılar, idari para cezalarının böyle bir halde dahi uygulanabileceğini iddia etmiştir. Ancak bir katılımcı, 5651 sayılı Kanun'un Anayasa Mahkemesi tarafından iptal edilen 6. maddesi 1. fıkrası d bendine atıfta bulunarak bu yolun işletilemeyeceğini beyan etmiştir. İlgili maddede internet servis sağlayıcıları. Bilgi Teknolojileri ve İletişim Kurumunun talep ettiği bilgileri, talep edilen şekilde kuruma teslim etmekle ve kurum tarafından bildirilen tedbirleri uygulamakla yükümlü tutulmuştur. Anayasa Mahkemesi, 8 Aralık 2015 tarihli kararında, talep edilen bilgiler arasında kişisel verilerin de bulunabileceği ve bu sebeple ilgili kişilerin bilgilendirilmesi gerektiğini belirtmiştir. Bu sebeple, soruşturmanın gizliliğini ihlal etmeme gibi kanunda açıkça tanımlanmış bir bilgilendirme yükümlülüğü bulunmadığı takdirde, internet servis sağlayıcısının idari yönden sorumlu tutulamayacağı ifade edilmiştir.

Fransa Ulusal Temas Noktası yetkilisi, uygulamada servis sağlayıcılarının işbirliği sayesinde benzer bir vakanın henüz ülkelerinde yaşanmadığını belirtmiştir. Operasyonel konularda kişileri bilgilendirmeme yükümlülüğünün Avrupa Birliği Genel Veri Koruma Düzenlemelerine (GDPR) uygun olduğu yönünde servis sağlayıcılarından geri bildirim aldıklarını da eklemiştir. İlgili kişiyi bilgilendirmek isteyen bir servis sağlayıcı olması durumunda ise durumun, talep eden ülke Temas Noktası'na bildirileceğini ve talep eden ülkenin isteğine göre sürecin şekilleneceğini ifade etmiştir. Ayrıca, Fransa'da yürüyen bir suç soruşturması yoksa ilgili kullanıcıya bilgilendirme yapılması halinde servis sağlayıcısının yasal sorumluluğunun doğmayacağını da beyan etmiştir. Letonya Ulusal Temas Noktası yetkilisi ise, Letonya Ceza Muhakemesi Kanunu uyarınca, servis sağlayıcıların işledikleri verilerin saklanmasından da sorumlu tutulduğunu belirterek gizli kalması gereken bilgilerin paylaşılması durumunda cezai sorumluluğun doğabileceğini ifade etmiştir.

2.8 Soru 8 – Verileri Silmeme Yükümlülüğü

A ülkesi, başka bir ülke Ulusal Temas Noktası'na bir veri saklama talebi gönderir. Gerekli işlemlerin ardından başlangıçta internet servis sağlayıcısı, talebin gereğini yapmayı kabul eder ve ilgili verilerin saklandığı konusunda temas noktasını bilgilendirir. Fakat adli istinabe talebi Türkiye'ye ulaştığında tüm verilerin geri döndürülemeyecek biçimde silindiği ortaya çıkar.

- **Bu durumda internet servis sağlayıcısının idari ve/veya cezai sorumluluğu nedir?**

- **Yasal sorumluluk açısından, verilerin kasıtlı veya taksirle silinmiş olması arasında herhangi bir fark var mıdır?**

Katılımcılar, taleple ilgili Türkiye'de yürüyen suç soruşturması bulunması halinde, idari sorumluluk yönünden, yukarıda da bahsi geçen 6698 ve 5651 sayılı Kanunlardaki yükümlülüklere aykırılık oluştuğundan idari para cezası verilebileceğinde görüş birliğine varmışlardır. Cezai sorumluluk açısından ise suç delillerini gizleme, yok etme ve değiştirmeye ilişkin Türk Ceza Kanunu'nun 281. maddesinin uygunluğu tartışılmıştır. İlgili maddede geçen, "gerçeğin meydana çıkmasını engellemek" özel kastının uygulamada gerçekleşmesinin veya gerçekleşse dahi ispat edilmesinin mümkün olamayacağı sonucuna varılmıştır. İnternet servis sağlayıcıları genellikle verileri, otomatik olarak silme ve yok etme işlemine gittikleri için ve Türk Ceza Kanunu'nun 281. maddesi taksirle işlenemeyeceğinden cezai sorumluluğun isnat edilemeyeceğini belirtmişlerdir.

Hâlihazırda Türkiye'de suç soruşturması bulunmaması durumunda, katılımcılar 7. soruya verdikleri cevapların (2. paragraf) bu senaryo için de genel olarak geçerli olduğunu belirtmişlerdir. Verilerin silinmesi eylemi, ancak Türk Ceza Kanunu'nun genel hükümlerine veya ilgili kanunlardaki idari yükümlülüklere aykırılık teşkil ediyorsa cezalandırılabilir.

Fransa Ulusal Temas Noktası yetkilisi, bazı durumlarda veri saklama talebi ileten ülkelerin adli istinabe sürecini başlatmadıkları için saklama talebine konu olan verilerin, servis sağlayıcılar tarafından silindiğini ifade etmiştir. Böyle bir halde, servis sağlayıcının yasal sorumluluğu bulunmamaktadır. Letonya Ulusal Temas Noktası yetkilisi ise, servis sağlayıcının saklamakla yükümlü olduğu verileri kasten silmesi durumunda Letonya Ceza Kanunu gereğince "delil yok etme" suçunun oluşacağını belirtmiştir.

2.9 Soru 9 - Tüzel Kişilerin Yükümlülükleri

Sözleşme'nin 12. maddesi, tüzel kişilerin yasal yükümlülükleri ile ilgilidir. Bahse konu veri saklama talebinin, büyük bir şirketin ağına dâhil belirli bir bilgisayara ilişkin olduğunu varsayalım. Şirket yöneticisi, saklama talebinin gereğini yapacağını resmi olarak Ulusal Temas Noktası'na bildirir. Fakat gerekli veri, ihtiyaç duyulduğunda orada değildir.

- **Türk hukuk sistemine göre, yükümlülükler açısından şirket yöneticileri ile internet servis sağlayıcıları arasında bir farklılık var mıdır?**

- **Şirket yöneticisinin veri saklama talebine olumlu yanıt vermemesi halinde Ulusal Temas Noktası, hangi yasal yollara başvurabilir?**

Katılımcılar, Sözleşme'nin 12. maddesinde vurgulanan tüzel kişilere ilişkin sorumluluğun, 5651 sayılı Kanun ile yükümlülük getirilen servis sağlayıcılar dışındaki özel hukuk tüzel kişilerini de kapsadığını belirtmiştir. Internet erişimine ilişkin veriler haricindeki verilerin tutulması, tüzel kişiler bünyesinde genellikle bilgi teknolojileri departmanlarının takdirine bırakılmış olup Ulusal Temas Noktası'nın saklama talebi yapması durumunda, ilgili şirketin hukuki sorumluluğunun açık bir biçimde tanımlanması gerektiği de eklenmiştir. Her ne kadar kişisel verileri koruma kanunu, tüzel kişilere verilerin işlenmesine ilişkin çeşitli sorumluluklar yüklemiş olsa da, ilgili hükümlerin saklama talebinin yerine getirilmesine yasal dayanak yapılamayacağı görüşü hakim olmuştur. Ayrıca, Sözleşme'nin 12. maddesi bağlamında, tüzel kişinin sorumluluğuna gidilebilmesi için iç hukukta gerekli düzenlemenin yapılmış olmasının ön şart olarak Sözleşme'de açıkça belirtildiği ifade edilmiştir.

Katılımcılar, tüzel kişilere cezai sorumluluk isnat edilemeyeceğine ilişkin Türk Ceza Kanunu 20. maddesine atıfta bulunmuşlardır. Ayrıca, iç hukukta yasal düzenlemeyle gerekli yükümlülük tanımlanmadığından dolayı, şirket yöneticisi tarafından Ulusal Temas Noktası'nın yapacağı veri saklama talebine olumsuz yanıt verilmesi halinde, Türk Ceza Kanunu'nun 133. maddesindeki güvenlik tedbirlerinin uygulanamayacağı konusunda da görüş birliğine varılmıştır. Bu sebeple, Ulusal Temas Noktası'nın, tüzel kişilerin veri saklama taleplerine uymalarını zorlayacak ya da sağlayacak yasal yol bulunmadığına kanaat getirilmiştir.

Fransa Ulusal Temas Noktası yetkilisi, veri saklama talebine ilişkin, yasal sorumluluk açısından internet servis sağlayıcıları ile şirket yöneticileri arasında fark bulunmadığını belirtmiştir. Letonya Ulusal Temas Noktası yetkilisi ise şirket yöneticilerinin sadece şirkette fiziksel olarak tutulan verilerden sorumlu olduğunu ifade etmiştir.

2.10 Soru 10 - İşbirliğinden Kaçınma

Muhtemel bir terör saldırısı ile ilgili olarak Ulusal Temas Noktası, A ülkesine acil bir talepte bulunur. Avrupa Konseyi Siber Suç Komisyonu tarafından yönetilen iletişim listesinde açıkça belirtilmesine rağmen, A ülkesinin yetkilileri ulusal temas noktamızı doğrulayamadığını iddia eder ve talebimizi, uzun bir zaman dilimi gerektirecek olan İnterpol iletişim kanalıyla göndermemizi ister. Bu esnada, terör saldırısı gerçekleşir ve telafisi güç ve imkânsız zararlar doğar.

- **Böyle bir durumda, başka bir ülkenin Temas Noktası'na karşı herhangi bir hukuki veya diplomatik süreç başlatmak mümkün müdür?**

- **A ülkesinin Temas Noktası'nın, Sözleşme'de belirtildiği gibi, 7/24 esasına göre takip etmesi gereken e-posta adresine veya telefon çağrılarına hiç cevap vermediğini veya çok geç yanıt verdiğini varsayalım. Bu senaryoda, uygulanacak hukuki yaklaşımda herhangi bir farklılığın olması mümkün müdür?**

Katılımcılar, Ulusal Temas Noktası'nın taleplere hızlı cevap verme yükümlülüğüne aykırı davranması veya hiç cevap vermemesi durumlarına karşı alınabilecek hukuki ve diplomatik tedbirlerde farklılık olmayacağını vurgulamışlardır. Senaryoda belirtilen duruma benzer bir olayın gerçekleşmesi halinde, ağırlıklı olarak diplomatik yollara başvurulabileceği hususunda görüş birliği oluşmuştur. Katılımcılar, Sözleşme'nin 45. maddesine atıfta bulunarak, iki üye ülke arasında uyuşmazlık oluşması durumunda konunun hakeme, Avrupa Suç Sorunları Komitesi'ne veya Uluslararası Adalet Divanı'na taşınabileceğini belirtmişlerdir. Her ne kadar düşük bir olasılık olsa dahi, meydana gelen zarar ile ilgili Ulusal Temas Noktası'nın ihmalkâr davranışı arasında bağ kurularak hukuki sorumluluk bağlamında zararın tazmini yoluna da gidilebileceği ifade edilmiştir. Böyle bir durumda, zararın meydana geldiği ülke yargı mercilerine mi yoksa yabancı ülke yargı mercilerine mi başvurulacağı konusunda tereddütler oluşmuştur.

Fransa ve Letonya Ulusal Temas Noktası yetkilileri, Interpol, Europol, elçilikler gibi böyle bir durumda kullanılabilecek diğer iletişim yollarının varlığına dikkat çekmişlerdir. Ayrıca, kasıtlı bir davranış sonucu zarar doğması halinde, diplomatik yollara başvurmanın da mümkün olduğunu eklemişlerdir.

2.11 Soru 11- Şüpheli Para Transferlerinin Durdurulması

A ülkesinde, mukim bir bankanın SWIFT sistemini zararlı yazılım kullanarak ele geçiren bir kişi, Türkiye'deki banka hesaplarına suçtan elde ettiği gelirleri gönderir. Bahse konu paranın hesaptan çekilmesini veya üçüncü bir ülkeye gönderilmesini engellemek için, A ülkesinin Temas Noktası ilgili banka hesaplarının ivedilikle dondurulmasını ve sonrasında da iade edilmesini talep etmektedir. Lütfen aşağıdaki soruları sırasıyla cevaplayınız.

Böyle şüpheli bir işlemde banka, bir hesabını savcılık talimatı veya mahkeme kararı olmaksızın kendi inisiyatifiyle dondurabilir mi?

- **Eğer cevabınız evet ise, azami ne kadar süre ile dondurabilir?**

- **Yargı kararı ulaşana kadar bankanın, hesabı, geçici olarak işleme kapattığını varsayalım. Bu esnada hesabın sahibi, parayı çekebilmek için bankayı hukuki süreç başlatmakla tehdit etmektedir. Bankanın hesap sahibine ve şüpheli işlemi bildiren kişilere karşı yetki ve sorumluluklarını etraflıca irdeleyiniz.**

- **Banka inisiyatif kullanıp hesabı dondurmazsa ve yabancı mağdurlar için geri dönüşü olmayan bir finansal kayba neden olursa, mağdurların zararını yasal yollardan telafi etmek mümkün müdür?**

- **Örnekteki gibi siber suç soruşturmalarında ilk müdahale aşamasında hukuka aykırı fiile ilişkin tüm delillerin toplanması çoğunlukla mümkün olmamaktadır. Yargı makamları, mağdur ülkenin elinde dolandırıcılığa ait yeterli kanıt bulunmadığı kanaatine vararak herhangi bir karar vermez ya da geçici dondurma tedbirinin kaldırılmasına karar verir. Finansal bir hakkın kullanılmasına sınırlandırılma getirilmesinin şartları ve sınırları, mevcut iç hukuk düzenlemelerine göre nedir? Bunları yeterli bulmuyor iseniz önerilerinizi paylaşınız.**

- **Her şey yolunda gider ve banka hesabı, uygun bir yargı kararıyla dondurulur. Ancak, soruşturmayla ilgili adli istinabe talebi Türkiye'ye gelmez. Banka, söz konusu hesabın tekrar kullanıma açılması için ne kadar beklemelidir? Sizce hesap, belirli bir süre sonunda kendiliğinden aktif hale mi gelmeli yoksa hesap sahibi, kişisel talepte mi bulunmalıdır?**

Katılımcılar, şüpheli işlem bildirimi üzerine bankaların, kişilerin hesaplarını dondurması üzerine birçok hukuki dayanak ileri sürmüşlerdir. Bankaların müşterileriyle yaptıkları genel nitelikli sözleşmelerde, hangi durumlarda hesapların banka tarafından doğrudan dondurulabileceğine ve kapatılabileceğine ilişkin maddeler olduğu ve uygulamada bankaların yoğunlukla böyle sözleşme kaynaklı yetkilere dayanarak işlem tesis ettikleri vurgulanmıştır. Hesapların banka tarafından ne kadar süreyle dondurulabileceği ise yine sözleşme hükümlerine bağlıdır ve süresiz olabilir. Ayrıca, 5549 sayılı "Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun"un 7. maddesi ile bankalara, şüpheli işlemlerde Mali Suçları Araştırma Başkanlığına (MASAK) bildirim yapma ve akabinde ilgili hesapları 7 gün süreyle dondurma yükümlülüğü getirildiği ifade edilmiştir. Bunlar haricinde, 5271 sayılı Ceza Muhakemesi Kanunu'nun 128. maddesi, 6415 sayılı "Terörizmin Finansmanının Önlenmesi Hakkında Kanun" ile 5411 sayılı Bankacılık Kanunu bağlamında da, banka hesaplarına el konulabileceği veya hesap sahibinin kullanımının sınırlandırılabileceği belirtilmiştir.

Yargı kararı alınana kadar banka tarafından resen hesabı dondurulan bir kişinin, yasal yollara başvurabileceği ifade edilmiştir. Bankayla sözleşme tarafı olmayan bir üçüncü kişinin zarara uğraması halinde, dondurulmayan o hesabın tamamı ile işlemiş faiz ve munzam zararlardan banka sorumlu olacaktır. Uygulamada bankalar, böyle ağır bir sorumluluğu almaktansa ilgili hesabı dondurup bu hesabın belli bir süre kullanılamamasından kaynaklı sorumluluğu tercih edeceklerdir. Hesabı dondurulan kişi, Borçlar Kanunu'ndaki haksız fiil hükümlerine dayanarak tazminat davası açabilecektir. Ancak birçok katılımcı, banka hesaplarının yasal olmayan saiklerle kullanılması halinde yargı makamlarının banka lehine karar vereceğini ve bu yüzden uygulamada hesap dondurma işlemlerine ilişkin hukuki ve cezai sorumluluğun doğmayacağını vurgulamışlardır. Benzer biçimde, Ulusal Temas Noktası'na şüpheli işlemi bildiren ve bankanın ilgili hesabı resen dondurmaması üzerine zarara uğrayan yabancı şahıslar da, tazminat yoluna başvurabileceklerdir.

Mahkeme kararıyla ilgili banka hesabının dondurulması tedbiri kaldırabilir ve bankanın bu karara karşı yasal yollarla direnme ihtimali bulunmamaktadır. Ayrıca böyle bir durumda, hesap sahibinin başvurusu aranmaksızın karar uygulanmalı ve hesap derhal kullanıma açılmalıdır. Mahkeme kararıyla tedbirin kaldırılmadığı durumda ise hesap sahibinin başvurusu durumunda mahkeme, aksi yönde karar almadıkça ilgili hesap kullanıma kesinlikle açılamaz.

Fransa Ulusal Temas Noktası yetkilisi, adli makamların emirleri haricinde kolluk kuvvetlerine, banka hesaplarını dondurma yetkisinin verilmediğini ifade etmiştir. Ayrıca hesap dondurma işleminin sadece şüpheli işleme konu olan para miktarıyla sınırlı olduğunu ve hesap sahibinin ilgili hesabı kullanmaya devam edebileceğini de eklemiştir. Bankalar, Fransa Parasal ve Mali Kanunu (COMFI) 561 ve 562. maddelerindeki istisnalar dışında, resen hesap dondurma işlemi yapamazlar. Bu tip istisnai hallerde, talep eden ülkenin mali suçlar biriminin Fransız

karşılığıyla temasa geçmesi ve ilgili talebin Fransız Bankalar Birliği (Interbank Community) tarafından uygun görülmesi şartları sağlandığında adli emir temin edilinceye kadar banka, resen hesap dondurma işlemi tesis edebilir. Ayrıca bankalar, uluslararası anlaşmalardan doğan yükümlülükleri gereği kendi aralarında da bu yolu işletebilirler. Bankaların, şüpheli işlem durum tespiti yükümlülüğüne uymamaları halinde LCBFT (Lutte Contre Blanchiment ve Financement du Terrorisme) gereğince mağdurlara karşı hukuki ve cezai sorumlulukları doğacaktır. Müşterinin, hesap dondurma işlemine yasal itiraz hakkı olup şüpheli işlemin hesap sahibinin iyi niyetli olduğu anlaşılırsa hesap dondurma sonucu doğan zararlar devlet tarafından karşılanır. Son olarak şüpheli işlem sonucu hesaba geçen paranın, talep eden ülkeye geri gönderilmesi ancak mahkeme kararıyla olduğundan adli istinabe sürecinin başlatılması gerekmektedir.

Letonya Ulusal Temas Noktası yetkilisi, şüpheli işlemlerde adli karar alınıncaya kadar bir banka hesabının 45 gün dondurulabileceğini belirtmiştir. Bu sürenin sonunda adli işlem tesis edilmemesi halinde, hesabın kendiliğinden kullanıma açılacağını da eklemiştir. Şüpheli işleme konu bir hesabın dondurulmaması sonucunda oluşan zararların, mağdurlar tarafından "Haksız Yolla Edinilmiş Mallara El Koyma Kanunu" kapsamında tazmini yoluna gidilebileceği ifade edilmiştir.

2.12 Soru 12 – Kolluk Kuvvetlerinin Şüpheli Banka Hesaplarını Resen Dondurması

Bazı ülkelerde kolluk kuvvetleri, kara paranın aklanması, terörün finansmanı ve acil durumlarda banka hesaplarını resen dondurabilmektedir.

- **Böyle bir olası yetkinin, Türk hukuk sistemine uygunluk bağlamında, kullanım şartları ve sınırları hakkında görüşlerinizi bildiriniz.**

- **Bilişim suçlarıyla etkin mücadele yapılabilmesi amacıyla yasal prosedürlerin hızlı bir şekilde aşılarak zamanında ve yerinde önleyici tedbir alınması açısından nasıl bir mevzuat ya da uygulama geliştirilebilir?**

Katılımcıların çoğu, acil durumlarda kolluğa banka hesaplarını resen dondurma yetkisinin verilebileceğini ifade etmişlerdir. Ancak Türk Ceza Hukuku sistemine uygun bir biçimde, böyle

bir yetkiye dayanarak alınan idari kararların 24 saat içerisinde yargı makamlarına sunularak etkili bir yargısal denetim yolunun öngörülmesi gerekliliğini de eklemişlerdir. Mevcut durumdaki uygulamalara da katılımcılar tarafından değinilmiştir. 5549 sayılı Kanun çerçevesinde bankalar, şüpheli işlemleri MASAK'a bildirmektedir. Azami 7 gün dondurulan banka hesapları için hazırlanan raporlar, Cumhuriyet Savcılıklarına iletilmektedir. Ceza Muhakemesi Kanunu'nun 128. maddesi kapsamında; soruşturma evresinde sulh ceza hakimi, kovuşturma evresinde mahkeme, gecikmesinde sakınca olan hallerde daha sonra yetkili hakime sunmak üzere Cumhuriyet Savcısı el koyma kararı almaktadır. Ayrıca katılımcılar, 6415 sayılı Kanun kapsamında oluşturulan idari bir kurulun da benzer yetkilerle donatıldığını ve mevcut uygulamalardan farklı olarak yargısal denetim dışında bırakıldığını işaret etmişlerdir.

Letonya Ulusal Temas Noktası yetkilisi, talep eden ülke Egmont grubunun bir üyesi ise suç gelirlerinin aklanmasına ilişkin taleplerin Letonya Finansal Suçlar Birimi'ne iletilmesi veya adli istinabe talebi gönderilmesi gerektiğini ifade etmiştir.

2.13 Soru 13 – Yabancı Mağdurlarun Resmi Şikayetlerinin Aranması

Türk Ceza Kanunu'nun 158. maddesi 1/f fıkrası uyarınca, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenen dolandırıcılık fiilleri temel suçun nitelikli hali olarak öngörülmüştür. Uygulamada, özellikle soruşturma aşamasının başında, yabancı mağdurların ifadeleri talep edilmekte ve temin edilmediği takdirde kamu davası açılmamaktadır. Bu pratiğin sebeplerini ve Türk hukuk sistemine uygunluğunu tartışınız.

Katılımcıların çoğunluğu, Türk Ceza Kanunu 158. maddesi 1/f fıkrası kapsamında işlenen suçların takibinin şikayete bağlı olmadığının altını çizerek mağdur ifadesi aranmadan resen soruşturma yürütülmesi gerektiğini ifade etmişlerdir. Bazı katılımcılar, mağduru veya şikayetçisi yurtdışında olan dosyalarda takipsizlik vermek gibi yanlış bir uygulama benimsendiğini de işaret etmişlerdir. Bir katılımcı ise karşı yönde görüş bildirmiştir. Dolandırıcılık suçunun oluşması için şüphelinin hile yapması ve müştekinin aldanması gerektiğini belirten katılımcı, mağdur ifadesi olmaksızın aldanma unsurunun oluşup oluşmadığına karar verilemeyeceğini ileri sürmüştür. Bu yüzden, mevcut uygulamanın Türk hukuk sistemine aykırı olmadığını dile getirmiştir.

2.14 Soru 14 - Saklama Süresi Dolan Verilerin Kullanımı

Türkiye'de, internet servis sağlayıcıları 5651 sayılı Kanun'a göre trafik verilerini 6 ay ile 2 yıl arasında saklamalıdır. Azami saklama süresi geçtikten çok sonra, ilgili adli istinabe talebinin ülkemize ulaştığını varsayalım. Ancak internet servis sağlayıcı, verileri silmemiştir ve yargı makamlarımız saklanan verileri, talebi yapan ilgili ülkeye göndermiştir.

a. Söz konusu şüpheli, bu verilerin artık kendisine karşı getirilen suçlamalarda delil olarak kullanılma vasfını yitirdiğini iddia eder ve bu nedenle mahkemede geçersiz olarak değerlendirilmesi gerektiğini savunur. Kişisel Verileri Koruma Hukuku ve Ceza Muhakemeleri Usul Hukuku bağlamında şüphelinin bu iddiasını irdeleyiniz.

b. Daha sonra şüpheli, internet servis sağlayıcısına kişisel verilerinin haksız yere tutulduğu gerekçesiyle dava açıyor. Ülkemizdeki hukuki düzenlemelere ve Avrupa Birliği Genel Veri Koruma Yönetmeliği'ne (GDPR) göre, servis sağlayıcının yasal sorumluluğu var mıdır?

c. Bu kez internet servis sağlayıcısı, korunan verileri maksimum saklama süresi sona erdiğinde otomatik olarak siler. Silme işleminden hemen sonra adli istinabe talebi ulaşır. Talepte bulunan ülke, bahse konu verilerin suç soruşturmasına ilişkin olduğu için kişisel verilerin koruma yükümlülüklerinden muaf tutulması gerektiği sebebi ile internet servis sağlayıcısını suçlayabilir mi? Kişisel Verileri Koruma Kanunu bağlamında, tesis edilen işlemde hukuka aykırılık var mıdır?

A şıkkında, saklama talebi yurtdışından geldiği için, talebi yapan ülkenin kanunlarınca azami yasal saklama süresi geçtikten sonra elde edilen verinin kabul edilip edilmediğine bakılması gerektiği değerlendirilmiştir. Alman Ceza Hukuku sisteminden örnek veren bir katılımcı, Almanya'da, ihlal edilen hak ile korunan hak arasında denge gözetilerek karar alındığını ve Türkiye'de azami saklama süresi geçtiği halde silinmeyen verilerin Almanya tarafından delil olarak kabul edilebileceğini ifade etmiştir. A şıkkındaki durumun Türkiye'deki bir şüpheliye uyarlanması halinde, yani başka bir ülkenin 2 seneden fazla sakladığı bir verinin mahkemeye ulaşması halinde, 5271 sayılı Ceza Muhakemesi Kanunu 217. maddesi gereğince delil, hukuka uygun elde edilmiş sayılmayacaktır. Bu hakim görüşe katılmayan bir katılımcı, delillerin saklandığı anda hukuka uygunluk halinin bulunduğu ve verilerin sahte olmadığı varsayımlarına

dayanarak azami veri saklama süresi geçse de delil vasfının kaybolmayacağını ileri sürmüştür. Ayrıca katılımcılar arasında azami süresinin ötesinde saklanan veriler için servis sağlayıcılarının Türk Ceza Kanunu'nun 138. maddesindeki "verileri yok etmeme" suçunu işleyecekleri konusunda çoğunluk görüşü oluşmuştur. Ancak bazı katılımcılar, 6698 sayılı Kanun'daki verileri yok etme ve verileri silme kavramları arasındaki farka dikkat çekerek karşı görüş bildirmiştir. Bahse konu kanuna dayanarak çıkartılan yönetmelikte, silme işlemi sonucunda ilgili verilere, veri işleyenler erişememekte, yok etme sonucunda ise hiç kimse erişememektedir. Katılımcı, veri işleyen tarafından Borçlar Kanunu'ndaki gibi verileri yok etmek için 10 senelik bir sürenin belirlenebileceğini ve 2 senenin sonunda silinen verilere, yargı makamları tarafından 10 seneye kadar ulaşılabileceğini önermiştir. Böylece veriler yok edilmediğinden servis sağlayıcılar, Türk Ceza Kanunu 138. maddesi kapsamında sorumlu tutulmayacak ve ayrıca yargı makamları uzun yıllar süren soruşturma ve kovuşturma evrelerinde dijital delillere erişme şansı elde edebileceklerdir. B şıkkında ifade edilen, 2 yıl sonunda silinmeyen/yok edilmeyen veriye ilişkin şüphelinin yasal hakları konusunda yapılan tartışmalar da bu eksende olmuştur. Katılımcıların çoğu "verileri yok etmeme" suçunun oluşacağını iddia ederken bir katılımcı, şirket politikasında şeffaf bir biçimde belirlenmesi ve örnek olaydaki gibi makul sebeplerin varlığı halinde, daha uzun süre verilerin saklanabilmesinin hukuka uygun olduğunu öne sürmüştür. C şıkkında ise servis sağlayıcının 5651 sayılı kanunda belirtilen sürelere riayet ettiği ve 2 yıllık süre sonunda ilgili verileri sildiği için yasal sorumluluğunun doğmayacağı konusunda tam bir görüş birliği hasıl olmuştur.

Letonya Ulusal Temas Noktası, dijital verilerin servis sağlayıcılar tarafından azami 18 ay saklandığını ve teorik olarak bu sürenin aşımından sonra ilgili verilerin şüphelilere karşı delil olarak kullanılamayacağını belirtmiştir. Yetkili, saklama süresi aşılmış dahi olsa verilerin delil niteliği taşıyıp taşımadığının karar merciinin adli makamlar olduğunu da eklemiştir ve böyle bir adli karar verilmesi durumunda servis sağlayıcısının hukuki ve cezai sorumluluğunun ortadan kalkacağını ifade etmiştir. Hukuka uygun kabul edilmeyen verilerin azami süre bittikten sonra saklanılması ve kullanılması halinde ise şüphelilerin yasal olarak itiraz yetkisi vardır; ancak uygulamada henüz benzer bir vaka gözlemlenmemiştir. Fransa Ulusal Temas Noktası yetkilisi bunlara ek olarak diğer ülkelerle paylaşılacak bilgilerin sınırının GDPR tarafından çizildiğini ve GDPR'ye aykırı davranış olması durumunda servis sağlayıcıların ağır yaptırımlarla karşı karşıya kalabileceği vurgulanmıştır.

2.15 Soru 15 – Trafik Verilerinin Gerçek Zamanlı Toplanması ve Kısmen Açıklanması

Sözleşme'nin 17. ve 20. maddeleri, tarafların trafik verilerini gerçek zamanlı olarak toplamasına ve kısmen paylaşmasına izin verir. Ayrıca, 21. madde, tarafların içerik verilerini elde etmelerine izin verir.

Organize bir suç topluluğunun, sadece üyelerinin eriştiği bir web sitesinin forumunda, yasadışı silah ticaretine ilişkin görüşmeler yaptığını varsayalım. Web sitesinin ülkemizde bulunan sunucusu, üyelerin iletişimi bittikten beş dakika sonra sohbetlerin verilerini otomatik olarak siler. A ülkesi, bu suç örgütünün ülkelerindeki üyelerini tanımlamak için trafik verilerine ihtiyaç duyar.

- **Hukuken, ülkemizde trafik verilerini gerçek zamanlı olarak toplamak ve bu bilgilerin yurtdışındaki şüpheli ve mağdurları tespit etmeye yardım olacak kısmını, diğer temas noktalarıyla acil yardım kapsamında paylaşmak mümkün müdür?**

- **Cevabınız olumlu ise, Ceza Muhakemesi Kanunu'nun 135. maddesinde sayılan suç türlerinde mi bu güvenlik tedbirini uygulama yetkisi vardır yoksa kapsamı daha geniş tutulabilir mi?**

- **Cevabınız olumsuz ise bu konuda nasıl bir mevzuat ve uygulama geliştirmek gerekir?**

Trafik verisinin gerçek zamanlı toplanmasının, Ceza Muhakemesi Kanunu'nun 135. maddesi kapsamında değerlendirilmesine ilişkin farklı teknik, organizasyonel ve yasal görüşler öne sürülmüştür. Katılımcıların çoğu, aynı maddede sayılan katalog suçlar haricindeki suçlar için iletişimin denetlenmesi tedbirinin alınamayacağını ileri sürmüşlerdir. Bir katılımcısı ise trafik verisinin, iletişimin içeriğine ilişkin bilgi barındırmadığından bahisle ilgili maddenin 5. fıkrasında tanımlanan iletişimin tespiti tedbirinin uygulanabileceğini belirtmiştir. Uygulamada HTS adıyla da bilinen ve telefon görüşmelerine ilişkin aranma bilgileri ile hedef telefon numaralarının bağlandığı baz istasyonları bilgilerini kapsayan iletişimin tespiti tedbiri, Ceza Muhakemesi Kanunu 135. maddedeki katalog suçlar haricinde de kullanılabilmektedir. Başka bir kullanıcı ise örnek olayda, 5 dakika dahi olsa sunucuda verilerin depolandığından hareket ederek durumun artık hukuken gerçek zamanlı iletişim olarak değerlendirilemeyeceği ve Ceza Muhakemesi Kanunu 134. maddesi kapsamında ilgili sunucuya el konularak adli bilişim incelemesi yapılması

gerekliliğine işaret etmiştir. Mevcut durumda yasal değişiklik yapılmadan, gerçek zamanlı trafik verisinin diğer Ulusal Temas Noktalarıyla kısmi paylaşımının dahi gerçekleştirilemeyeceği ve adli istinabe yolunun işletilmesi zorunluluğu ifade edilmiştir. Teknik ve organizasyonel açıdan ise katılımcılar, yerli ve yabancı içerik sağlayıcılarının gerçek zamanlı trafik verisini toplamak için yeterli teknik kabiliyetlerinin veya işbirliği niyetlerinin olmaması ile yaygın olarak kullanılan bulut bilişim çözümleri yüzünden farklı ülkelere dağılmış veriler ve uygulamalar olmasını en büyük engeller olarak tanımlamışlardır. Bir katılımcı, buluttaki verilere adli bilişim incelemesi için erişilmesi hakkında, Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi ile uzak bilgisayar kütüklerinin aranmasına ve yedeklenmesine dair kolluğa yetki verildiğini; ancak Ceza Muhakemesi Kanunu'nda benzer bir yetkilendirme olmadığı için, bu konunun yasal açıdan tartışmalı ve ulusal egemenlik bağlamında sakıncalı olduğunu eklemiştir.

Fransa ve Letonya Ulusal Temas Noktası yetkilileri ülkelerinde trafik verilerini gerçek zamanlı olarak toplamanın mümkün olduğunu ifade etmişlerdir. Fransa iç hukuku, terör ve organize suçlarla mücadele soruşturmalarında bu tedbire cevaz verirken bir servis sağlayıcıdan düzenli olarak talep edilen trafik verisini de kişisel veri olarak değerlendirmemektedir.

2.16 Soru 16 – İçerik Verileri İçin İletişimin Denetlenmesi Tedbiri

Başka bir organize suç grubunun, küçük çocukların cinsel görüntülerini VoIP (Voice-over-IP) teknolojileri aracılığıyla para karşılığında canlı olarak satmaya zorladığını varsayınız (Webcam Child Prostitution/Live Streaming Child Abuse on Demand). Geleneksel suçlardan farklı olarak mağdur ile şüpheli arasındaki görüntülü sohbet, hem suç fiilini hem de suç kanıtını oluşturan tek unsur olmaktadır. Taraflardan biri, görüşmeyi değişik uygulamalarla kaydetmediği müddetçe, suç fiiline ilişkin başkaca delil bulmak mümkün olmamaktadır. Bu örnekte, mağdurlar ve failler farklı ülkelerde; ancak ilgili VoIP servisinin sunucusu ülkemizde bulunmaktadır. VoIP hizmetleri, kişilerin haberleşme hak ve hürriyetleriyle yakından ilgili olduğu için internet servis sağlayıcı, sadece abone kimlik verisini otomatik olarak toplamaktadır. A ülkesi, mağdurları tespit etmek ve canlı çevrimiçi çocuk istismarının tek kanıtını ortaya çıkarmak amacıyla, belirli bir şüpheli için içerik verilerini gerçek zamanlı olarak toplamamızı ve kendileriyle paylaşmamızı talep eder.

- **Mevcut durumda, bütün ülkelerin, iletişimin denetlenmesi için yasal yetkileri bulunmaktadır. Türk hukuk sistemine göre, Ceza Muhakemesi Kanunu 135. ve 140. madde başta olmak üzere, çevrimiçi ortamlarda bu tür bir güvenlik tedbiri almak**

için yeterli bir yasal dayanak var mıdır?

- **A ülkesinde yaşanabilecek olası fiziksel çocuk istismarını engellemek adına, istisnai tedbirlerle elde edilmiş bu verilerin hızlıca paylaşımı mümkün müdür?**

- **Yasal dayanağın olduğunu/oluşturulduğunu ve gerekli yargı kararının ilgili servis sağlayıcısına bildirildiğini varsayalım. Servis sağlayıcı, VoIP sisteminin kendileri de dâhil üçüncü bir tarafın müdahalesini imkânsız kılacak biçimde, uçtan uca şifreleme (end-to-end encryption) ve eşler arası dağıtık ağ (P2P Distributed Network) prensiplerine dayandığını belirterek, yargı kararına uyulmasının fiilen imkânsız olduğunu belirtir. Böyle bir durumda uygulanabilecek pratik ve yasal düzenlemeler hakkında lütfen görüşünüzü bildiriniz.**

Katılımcılar, gerçek zamanlı içerik verisinin toplanmasının teorik olarak Ceza Muhakemesi Kanunu 135. maddesi çerçevesinde yapılabileceğini; ancak uygulamada bunu imkansız hale getiren teknik ve pratik koşullar bulunduğunu ifade etmişlerdir. Bir katılımcı ise iletişime ilişkin veri şifrelendiği için, Ceza Muhakemesi Kanunu 134. maddesi kapsamında da işlem tesis edilebileceğini ileri sürmüştür. Ayrıca başka bir katılımcı, hangi teknik koşullar bir arada sağlandığında, merkezi yurtdışında olan popüler VoIP (Voice-over-IP) uygulamalarının ve sosyal medya platformlarının Türkiye'de üretilen içeriklerine müdahale edilebileceğini detaylı bir biçimde anlatmıştır. Buna göre, bahse konu uygulamaların ürettiği içeriklerin ve trafiğin Türkiye içindeki sunuculara yönlendirilmesi ve tutulması ile bu yazılımların kaynak kodlarının elde edilmesi şartlarının beraber gerçekleşmesi gerekmektedir. Birçok katılımcı böyle bir ihtimalin çok uzak olduğunu ve ayrıca hayata geçirilse dahi uygulamada istenen etkiyi yaratamayacağını işaret etmişlerdir. Moderatör, son yıllarda şiddetlenen şifreleme tartışmasından genel olarak bahsetmiş ve uygulamalara kolluk kuvvetlerinin belli durumlarda erişim sağlaması, iletişimde kullanılan özel anahtarların bağımsız bir kurumda tutulması ve yasal düzenlemelerle servis sağlayıcılarına bilgi verme yükümlülüğü getirilmesi hususlarında kısa bir bilgilendirme yapmıştır. Ancak katılımcıların çoğu, an itibariyle yüzlerce benzer iletişim uygulaması olduğunu ve kullanıcıların hızlı bir biçimde alternatif uygulamalara yöneleceklerini hatta yeni teknolojik çözümler dahi geliştirebileceklerini vurgulamıştır.

Katılımcılar, şüphelinin ve mağdurun tespiti ile devam eden istismar vakasını önlemek adına gerçek zamanlı içerik verisinin paylaşılması noktasında, hem Sözleşme metninde hem iç hukukta yasal düzenleme eksikliğinin bulunduğunu belirtmişlerdir. Bu sebeple önce saklama talebinin yapılmasının ve daha sonra adli istinabe talebi ulaştığında bilgi paylaşımında bulunulmasının daha uygun olacağı değerlendirilmiştir. Bir katılımcı, sözleşmenin örnekteki gibi ciddi olaylarda

bilgi paylaşımına izin verdiğini ve iç hukukta gerekli yasal düzenlemeler yapılırsa mahkeme kararıyla sınırlı bir kapsamda istihbari bilgi paylaşımının mümkün olabileceğini vurgulamıştır. Aynı katılımcı, mevcut mevzuatın böyle hızlı müdahaleler yapmaya müsait olmadığını da dile getirmiştir. Başka bir katılımcı ise iletişim içeriklerinin ve bunların dökümlerinin özel usullere tabi olduğunu ve içeriğin paylaşılması halinde, özellikle imha yükümlülüğüne uyma bağlamında sıkıntılar yaşanabileceğine dikkat çekmiştir.

2.17 Soru 17 - Kendiliğinden Bilgi Verme

İstihbarat birimleri, A ülkesinde yaşayan iki terör örgütü üyesi arasındaki sohbet kayıtlarını elde eder. Konuşmalar, bu iki kişinin, ülkemizde bulunan bir havaalanına saldırı planı yaptıklarını işaret etmektedir.

- **Sözleşme'nin 26. maddesi, taraflara resen bilgi gönderme hakkı verir. İstihbarat kaynaklı bilgilerin de bu çerçevede değerlendirilebileceğini ve paylaşılabileceğini düşünüyor musunuz? Yoksa bu madde sadece suç soruşturmaları ve kovuşturmaları kapsamında mı değerlendirilmelidir?**

- **A ülkesinin de aynı bilgiyi istihbarat birimince muhbirler kanalıyla elde ettiğini varsayalım. A ülkesi, internet servis sağlayıcısı ile irtibata geçer ve bahse konu iki teröristin abone kimlik bilgilerini alır. Ancak A ülkesi, Ulusal Temas Noktası'na konu ile ilgili herhangi bir bilgi vermez. Ölümcül bir saldırının ardından, internet servis sağlayıcısı aracılığıyla Ulusal Temas Noktası, A ülkesinin bu olaydaki ihmalini öğrenir. A ülkesine karşı, ne tür yasal ve diplomatik adımlar atılabilir?**

Katılımcıların çoğu, Sözleşme'nin 26. maddesinin istihbari nitelikte bilgi paylaşımına da izin verdiği yönünde görüş bildirmiştir. Bir katılımcı, karşılıklılık ve iyi niyetin uluslararası hukukta hakim ilkeler olduğundan bahisle, bu evrensel ilkelerin çizdiği sınırlar çerçevesinde her türlü suç soruşturmasına veya istihbari nitelikteki çalışmaya ilişkin bilgi paylaşımı yapılabileceğini vurgulamıştır. Bazı katılımcılar, Sözleşme'de geçen "soruşturma (investigation)" ifadesinin istihbari faaliyetleri dışlayabileceğini belirtmiştir. Moderatör, ülkemizdekinin aksine birçok ülkede istihbari bilgi toplama faaliyetlerinin de suç soruşturması kavramı içerisinde değerlendirildiğini eklemiştir. Karşı görüş bildiren bir katılımcı, 26. maddede öngörülen paylaşıma ilişkin bilginin

bir suç soruşturmasından elde edilmesi gerektiğini ifade etmiştir. Bahse konu suç soruşturmasının da sözleşmenin 2. ve 11. maddeleri arasında tanımlanan siber suçlara ilişkin olması gerektiğini ve örnekteki gibi bir terör olayı için 26. madde kapsamında diğer Ulusal Temas Noktalarına bilgi verilemeyeceğini eklemiştir. Kritik bilgilerin paylaşılmaması neticesinde zarar doğması üzerine katılımcılar, değişik görüşler bildirmişlerdir. Bazı katılımcılar, yabancı temas noktaları için diplomatik kanalların, Ulusal Temas Noktası için ise Türk Ceza Kanunu'ndaki "görevi ihmal" gibi genel maddelerin işletilebileceğini ifade etmişlerdir. Bir katılımcı ise, ilgili maddenin Ulusal Temas Noktası'na yükümlülük getirmediği ve paylaşım yapma noktasında takdir yetkisi tanıdığını belirterek herhangi bir cezai sorumluluğun doğmayacağını ileri sürmüştür.

Letonya Ulusal Temas Noktası yetkilisi, Letonya kanunlarının istihbari bilgi paylaşımına izin verdiğini belirterek bu yetkinin servis sağlayıcıları ve Ulusal Temas Noktası açısından sınırlarını çizmiştir. Gecikmesinde sakınca duyulan ve telafisi güç veya imkansız zararlar doğurabilecek hallerde, servis sağlayıcı ve Ulusal Temas Noktası, bunu engelleyecek ölçüde bilgi aktarımı yapabilir. İhtiyaç duyulandan fazla bilginin verilmesi veya diğer suistimal biçimlerinde, kişisel verilerin korunması yönünde hukuki ve cezai sorumluluk doğacaktır. Fransa Ulusal Temas Noktası yetkilisi ise, Sözleşme'nin lafzi hükmüne dikkat çekmiş ve istihbari bilgi paylaşımının bir zorunluluk olmadığını belirtmiş ve Interpol gibi alternatif iletişim kanallarının varlığına dikkat çekmiştir.

2.18 Soru 18 - İnternet Servis Sağlayıcıları ile Daha Etkin İşbirliği

Türkiye, ikili ve çok taraflı anlaşmalar kapsamında diğer ülkeler ve Interpol gibi uluslararası polis organizasyonları ile uluslararası polis işbirliği faaliyetleri düzenlemektedir. Ancak Budapeşte Sözleşmesi, dijital delillerin ivedilikle muhafaza edilmesi ile mağdur ve şüpheli şahısların hızlıca tespit edilmesi amaçları başta olmak üzere geleneksel yöntemlerden daha hızlı karar alma ve bilgi paylaşımı yollarını öngören istisnai bir metindir. Sözleşme'nin öngördüğü şekilde etkin bir uluslararası polis işbirliğinin uygulanabilmesi ve en hızlı şekilde bilgi/veri paylaşımının yapılabilmesi için hukuki ve organizasyonel çözüm yolları açısından aşağıdaki konularda görüşlerinizi bildiriniz.

- **Bazı ülkelerdeki Ulusal Temas Noktaları, ülke içindeki tüm yerel servis sağlayıcılar ile çoğunlukla e-posta yoluyla olmak üzere hızlı iletişim kanallarına sahiptir. Böyle bir sistemin, ülkemizde kurulması, yasal ve idari açıdan mümkün**

müdür? Değil ise hangi değişikliklerin yapılması gerekmektedir?

- **Ulusal Temas Noktası, bazı yabancı internet servis sağlayıcılarından doğrudan bilgi temin edebilmektedir. Ayrıca Avrupa Birliği'ne üye ülke polis teşkilatlarının, diğer üye ülkelerde bulunan internet servis sağlayıcılarından doğrudan bilgi talep edebilmesine olanak sağlayan bir yasa tasarısı tartışılmaktadır. Bu kapsamda, yabancı bir güvenlik biriminin, Türkiye'de mukim bir internet servis sağlayıcısından doğrudan bilgi talep edebilmesinin uygunluğunu, şartlarını ve sınırlarını belirtiniz.**

Moderatör, uygulamada ABD merkezli bazı internet servis sağlayıcılarının doğrudan yabancı kolluk kuvvetlerine abone kimlik bilgisi sağlayabildiğini ve ayrıca ABD merkezli internet servis sağlayıcıları ile ABD Ulusal Temas Noktası arasındaki iletişimin yoğunluklu e-posta üzerinden gerçekleştiğini ifade ederek tartışmayı başlatmıştır.

Katılımcıların tamamı, Türkiye merkezli servis sağlayıcılarından, yabancı Ulusal Temas Noktası'na doğrudan bilgi akışı olması noktasındaki endişelerini bildirmişlerdir. ABD merkezli internet servis sağlayıcılarının ticari kazanç saikiyle hareket ettiği için bu tip doğrudan iletişim kanalları oluşturduğunu iddia eden bir katılımcı, Türkiye merkezli servis sağlayıcılarının ABD veya diğer ülkelerde benzer büyüklükte müşteri kitlesi olmadığı için böyle bir uygulamaya ihtiyaç duyulmayacağını ileri sürmüştür.

Katılımcıların büyük çoğunluğu, uluslararası paylaşıma konu olan bilginin karşılıklılık, ülkenin dış politikası ve iç hukuka uygunluk gibi birçok hassas değerlendirmeye tabi tutulması gerektiğinden bahisle, yargısal ve diplomatik kanalların tamamen devre dışı bırakılmasının sakıncalı olacağını belirtmiştir. Bir katılımcı, muhtemelen ABD merkezli internet servis sağlayıcılarının da ülke içindeki yetkilileri sıklıkla bilgilendirdiklerini ve benzer bir uygulamanın Türkiye için hayata geçirilmesi durumunda, doğrudan bilgi paylaşımına ilişkin dışsal denetim mekanizmasının da düzenlenmesi gerekeceğini vurgulamıştır. Başka bir katılımcı ise bahse konu yetkinin, ülkelerin egemenlik haklarıyla doğrudan ilişkili olduğundan hareketle uluslararası bir sözleşmeye dayanarak üye ülkelerin karşılıklı olarak böyle bir yetki tanıması haricinde, tek taraflı olarak iç hukukta yapılan bir yasal düzenlemenin yeterli olmayacağını belirtmiştir.

Yurt içinde, Ulusal Temas Noktası ile Türkiye merkezli servis sağlayıcıları arasında e-posta yoluyla daha hızlı iletişim kurulması gerekliliğini tüm katılımcılar kabul etmişlerdir. Bazı katılımcılar, servis sağlayıcılarının hassas kişisel verilerle ilgilendiğini vurgulamışlar ve Ulusal Temas Noktası'yla paylaşılacak verilerin içeriğine ilişkin detaylı bir yasal düzenlemenin zorunlu olduğunu eklemişlerdir. Bir katılımcı ise özellikle saklama taleplerinin, vakit kaybetmeksizin icrası

için e-posta yoluyla bilgi iletiminin artık bir seçenek değil mecburiyet haline geldiğini belirtmiştir. Teknik yönden ise iki taraf arasındaki iletişimin güvenliğini azami seviyeye çıkartmak için Kayıtlı E-Posta (KEP) veya Ulusal Yargı Ağı Projesi (UYAP) gibi güvenilir sistemler üzerinden, önceden tanımlanmış e-posta adresleriyle bilgi paylaşımının yapılmasının uygun olacağı görüşü ağırlık kazanmıştır.

3 Sonuç

Çalıştay, farklı uzmanlık alanlarından gelen katılımcıların çeşitli görüşlerine sahne olmuştur. Ancak etkinlik boyunca bazı konular birçok katılımcı tarafından defaatle vurgulanmıştır. Sözleşme'nin ruhen ve lafzen, iç hukuka etraflıca uyumlandırılması gerekliliği, uzmanların çoğu tarafından ifade edilmiştir. Sözleşme; abone kimlik verisi, trafik verisi ve içerik verisi şeklinde üçlü bir ayrıma giderken Türk hukukunda abone kimlik bilgisi, trafik verisinin bir parçası olarak tanımlanmakta olup içerik verisi ise henüz tamamlanmamıştır. Benzer biçimde 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" yasal sorumluluklar açısından erişim, yer, içerik ve toplu kullanım sağlayıcıları olarak dörtlü bir ayrıma giderken Sözleşme Servis Sağlayıcıları kavramından başka bir tabir kullanmamıştır. Özellikle çalıştayın ilk gününde, Sözleşme ve iç hukuk arasındaki bu tanımsal farklılıklar, kavram karmaşasına ve yanlış yorumlamalara yol açmıştır.

Etkinlikte sıklıkla ifade edilen diğer bir husus ise, Ulusal Temas Noktası ile internet servis sağlayıcılarının görev ve yetkilerinin kapsamının yasal düzenlemeler ile netleştirilmesiydi. Saklama talepleri ve acil durumlarda uluslararası bilgi paylaşımı hususlarında, katılımcıların geneli tarafından sadece Sözleşme'ye dayanılması yeterli bulunmamıştır. Bunlara ilişkin yasal altyapının yeni düzenlemelerle sağlamlaştırılması, yurtiçinde Sözleşme'ye uygun hareket edilmesinin önemli bir ön koşulu olarak ifade edilmiştir.

4 Katılımcı Listesi

Moderatör

Kemal Veli AÇAR	Şube Müdürü	EGM-Siber Suçlarla Mücadele Daire Başkanlığı

Katılımcılar

Erdal ÇETİNKAYA	Daire Başkanı	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
Kerim ALTIAY	Daire Başkan Yardımcısı	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
İbrahim ÖZDEMİR	Komiser	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
Murat Volkan DÜLGER	Doçent Doktor	İstanbul Aydın Üniversitesi
Hasan SINAR	Doçent Doktor	Altınbaş Üniversitesi
Yavuz ERDOĞAN	Doçent Doktor	Lefke Avrupa Üniversitesi
Özgür KARLITEPE	Siber Suçlarla Mücadele Şube Müdürü	EGM-İstanbul Emniyet Müdürlüğü
Mehmet PAKİŞ	Hakim	Yargıtay Başkanlığı
Ömrü YILMAZ	Hakim	Yargıtay Başkanlığı
Ayla SERÇE	Uzman Yardımcısı	Adalet Bakanlığı-Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü
Mehmet YILDIZ	Emniyet Amiri	EGM- İnterpol-Europol Dairesi Başkanlığı
Mahmut Kaan YÜKSEL	Savcı	Ankara Cumhuriyet Başsavcılığı
Murat SEMİZ	Savcı	İstanbul Cumhuriyet Başsavcılığı
Baki Çağrı ONGUN	Hakim	İstanbul Hakimi
Soner KAYA	Savcı	İzmir Cumhuriyet Başsavcılığı
Enes Koray KOÇAK	Komiser	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
Kadir BAĞCI	Hakim	Adalet Bakanlığı
Ceren KÜPELİ	Avukat	Turkcell İletişim Hizmetleri A.Ş.
Burhanettin AL	Avukat	Turkcell İletişim Hizmetleri A.Ş.

Ayşe ŞEKER	Avukat	Türk Telekominikasyon A.Ş.
Çağrı YALÇIN	Avukat	Türk Telekominikasyon A.Ş.
Osman Özkan NAZLIM	Polis Memuru	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
Mustafa SAĞLAM	Polis Memuru	EGM-Siber Suçlarla Mücadele Daire Başkanlığı
Gökhan BOZDOĞAN	Teknoloji ve Güvenlik Operasyonları Müdürü	Vodafone A.Ş.
Sait REÇBER	Mahremiyet Müdürü	Vodafone A.Ş.
Emre ERGİN	Avukat	Vodafone A.Ş.
Yeliz KILIÇ	Avukat	İçişleri Bakanlığı - Hukuk Müşavirliği
Muhammed DÜLGERLER	Avukat	İsimtescil A.Ş.
Engin PURCU	Polis Memuru	EGM-İstanbul Emniyet Müdürlüğü
Müşerref ÇUHADAR	Komiser Yardımcısı	EGM-Dış İlişkiler Dairesi Başkanlığı
Ali Rıza ÇELİK	Emniyet Amiri	EGM-Dış İlişkiler Dairesi Başkanlığı
Mehmet UÇAR	Bilgi Teknolojileri Yöneticisi	İsimtescil A.Ş.
Özgür ÖZCAN	Sistem Müdürü	Mynet.com A.Ş.

Bilgi Teknolojileri ve İletişim Kurumu'ndan iki uzman*

Adalet Bakanlığı'ndan bir uzman*

Turkcell İletişim Hizmetleri A.Ş.'nden bir uzman *

Yabancı Konuklar

Fransa 7/24 Ulusal Temas Noktası Yetkilisi*

Letonya 7/24 Ulusal Temas Noktası Yetkilisi*

Romanya 7/24Ulusal Temas Noktası Yetkilisi*

* Katılımcı, çalıştay raporunda isminin yer almasını istemedi.

İncek Mahallesi Boztepe Sk. 06830 Gölbaşı / Ankara
0 312 462 55 00
0 312 286 92 06
siber@egm.gov.tr