

TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ

24

YASAMA YILI

2

**(10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU
BİLGİ TOPLUMU OLMA YOLUNDA BİLİŞİM
SEKTÖRÜNDEKİ GELİŞMELER İLE
İNTERNET KULLANIMININ BAŞTA
ÇOCUKLAR, GENÇLER VE AİLE YAPISI
ÜZERİNDE OLMAK ÜZERE SOSYAL
ETKİLERİNİN ARAŞTIRILMASI AMACIYLA
KURULAN MECLİS ARAŞTIRMASI
KOMİSYONU**

TUTANAK DERGİSİ

29 Mayıs 2012 Salı

**(10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU BİLGİ TOPLUMU
OLMA YOLUNDA BİLİŞİM SEKTÖRÜNDEKİ GELİŞMELER İLE
İNTERNET KULLANIMININ BAŞTA ÇOCUKLAR, GENÇLER VE
AİLE YAPISI ÜZERİNDE OLMAK ÜZERE SOSYAL ETKİLERİNİN
ARAŞTIRILMASI AMACIYLA KURULAN MECLİS ARAŞTIRMASI
KOMİSYONU**

GÖRÜŞME TUTANAKLARI

29 Mayıs 2012 Salı

----0----

K O N U

İnternet Kullanımı hakkında

Sayfa
1:21

İÇİNDEKİLER

<u>İİ</u>	<u>Sayfa</u>
BİRİNCİ OTURUM	1:21
Dr. Mustafa TAŞKIN (Adalet Bakanlığı Kanunlar Genel Müdürlüğü Daire Başkanı)	1:3, 20:21
Dr. Nurdan OKUR (Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürü)	4, 18, 20
Mustafa SABİT (Adalet Bakanlığı Tetkik Hâkimi)	5:7, 15:16
Mesut ORTA (Adalet Bakanlığı Bilgi İşlem Dairesi Başkanı)	8, 9:12, 13, 14:15, 19
Haydar AKAR	Kocaeli 8, 13:14, 15, 16
Aytuğ ATICI	Mersin 12
Levent KURT (Uluslararası Hukuk ve Dışilişkiler Genel Müdürlüğü Daire Başkanı)	17:18, 19
Erdal AKSÜNGER	İzmir 20, 21

Açılma Saati: 15.20

Kapanma Saati: 16.32

29 Mayıs 2012 Salı

BİRİNCİ OTURUM

Açılma Saati: 15.20

BAŞKAN: Necdet ÜNÜVAR (Adana)

BAŞKAN VEKİLİ: Yıldırım M. RAMAZANOĞLU (Kahramanmaraş)

SÖZCÜ: İlhan YERLİKAYA (Konya)

KÂTİP: Erdal AKSÜNGER (İzmir)

----- 0 -----

BAŞKAN – Bilişim ve İnternet Araştırma Komisyonumuzun çok değerli üyeleri, değerli konuklarımız, değerli uzmanlarımız, değerli basın mensupları; hepinizi saygıyla selamlıyorum.

Perşembe akşamından dün akşama kadar Bilişim ve İnternet Araştırma Komisyonu olarak İstanbul’da gerçekten son derece verimli toplantılar yaptık, ziyaretler yaptık.

Bilişim ve mobil İnternet sektörünün önde gelen kuruluşlarını, yaklaşık on tane kuruluşu ziyaret ettik. Bakırköy Ruh ve Sinir Hastalıkları Hastanesinde İnternet bağımlılığıyla ilgili kliniği ziyaret ettik. İki tam gün, cumartesi, pazar günü bilişim ve İnternet sektörünün hemen hemen bütün aktörlerinin katıldığı iki günlük fevkalade verimli bir çalıştay yaptık. Ön raporlar gerçekten son derece doyurucu. Keza, içerik sağlayıcılar, İnternet’e reklam verenler ve e-ticaret siteleri, yaklaşık yirmi bir tane siteydi, o sitelerle sabahtan öğleye kadar çok önemli, verimli bir ziyaret yaptık. En son İstanbul Emniyet Müdürlüğü MOBESE Merkezini, Komuta Kontrol Merkezi ve Bilişim Laboratuvarını ziyaret ettik, gerçekten dolu dolu bir dört gün. Neredeyse üyelerimiz ve uzmanlarımızın nefes almadan takip ettiği bir dört gün geçirdik ama yoğun bir şekilde çalışmaya devam ediyoruz. Bugün Adalet Bakanlığımızdan üç ayrı birimin sunumunu dinleyeceğiz ve ondan sonra da tartışmaya açacağız.

Bugünkü sunumu basın mensubu arkadaşlardan özür dileyerek basına kapalı yapmak istiyoruz, o yüzden bizi bağışlasınlar. Biz daha sonra inşallah basına gereken bilgi notunu göndereceğiz.

Evet, basın mensubu arkadaşlar, çok teşekkür ediyorum.

Değerli Adalet Bakanlığı yetkilisi arkadaşlarım, sizden de özellikle rica ediyorum, Meclisin yoğun bir çalışma takvimi var, o yüzden mümkün olduğunca seri şekilde sunumlarımızı yapabilirsek -zaten sunumlarınız var- çok mutlu oluruz hem de Meclis çalışmalarını da aksatmamış oluruz.

İlk sunumu Adalet Bakanlığı Kanunlar Genel Müdürlüğü yetkilisi arkadaşlardan Kişisel Verilerin Korunması Kanunu Tasarısı ve Ulusal Bilgi Güvenliği Kanun Tasarısı çalışmaları hakkında alacağız.

Buyurunu Sayın Taşkın.

ADALET BAKANLIĞI KANUNLAR GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI DR. MUSTAFA TAŞKIN – Sayın Başkan, Komisyonumuzun değerli vekilleri; hepinizi en içten saygılarımla selamlıyorum.

Ben Adalet Bakanlığı Kanunlar Genel Müdürlüğünde Daire Başkanı olarak görev yapıyorum. Bugün sizlere bir on-on beş dakikalık süre zarfında Kişisel Verilerin Korunması Kanun Tasarısı ve Ulusal Bilgi Güvenliği Kanun Tasarısı hakkında kısa arzda bulunacağım.

Öncelikle “Kişisel Verilerin Korunması Hakkında Kanuna niçin ihtiyaç var?” konusunda birkaç cümle sarf etmek istiyorum.

Hepinizin malumu, kişisel veriler, insanların, bireylerin isimlerinden, iletişim bilgilerinden mali bilgilerine kadar, sağlık özgeçmişlerine kadar, ailevi bilgilerine kadar çok geniş bir alandaki bilgileri ihtiva ediyor ve bu bilgiler gününüzde özellikle otomatik yollarla bilişim sistemleri üzerinden çok yoğun bir şekilde kullanılıyor. Bu kullanım hem özel sektör bakımından hem kamu sektörü bakımından oldukça yaygın. Bu alanda ülkemizde şu an için birtakım yasal boşluklar söz konusu. Örneğin, Türk Ceza Kanunu’nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak işlenmesi, kullanılması hâli suç olarak düzenlenmiş olmasına rağmen hangi hâllerde hukuka uygun, hangi hâllerde hukuka aykırılık söz konusu olduğu konusunda belirsizlikler var. O yüzden “Kişisel Verilerin Korunması Hakkında Kanun” a ihtiyaç var.

Yine, geçtiğimiz 2010 yılında Anayasa değişikliğiyle bireylere temel bir hak olarak bu hak tanındı, Anayasa gereği de bizim bu kanunu çıkarmamız gerekiyor. Diğer taraftan, Avrupa Birliği müzakere sürecinin dört tane faslıyla doğrudan alakalı bir konu kişisel verilerin korunmasına ilişkin süreç.

Yine, Europol, EUROJUST, Sirene Ofisi, Schengen Bilgi Sistemi gibi güvenlik birimlerimizin ve yargı birimlerimizin çok sık irtibat hâlinde olduğu bu mekanizmalarla iş birliği bakımından da kişisel verilere ilişkin bir kanunumuzun olmaması sebebiyle ciddi sorunlar yaşanıyor. Öte yandan, sermaye bakımından, ekonomi bakımından da kişisel veriler son derece önemli bir hâle geldi, zira ülkemiz ekonomik bakımdan son derece hızla büyüyor ve uluslararası yatırımlar yapıyorlar. Ancak bu uluslararası yatırımlarının olduğu bölgelerde değil de burayı İstanbul’dan, Ankara’dan yönetmek istediklerinde oradaki verileri Türkiye’ye alamadıklarından dolayı yönetim sıkıntıları yaşıyorlar ve yönetim merkezlerini Polonya’ya, Romanya’ya veya yatırım yaptıkları ülkelere taşımak zorunda kalıyorlar. Bunun daha detayları var ancak süre sıkıntısı sebebiyle bunları geçiyorum.

Tüm bu gerekçelerle kişisel verilerin korunmasına ilişkin bir süreç başlatıldı, tarihi 1989 yılına kadar dayanıyor, en son 2006 yılında Sayın Profesör Doktor Bahri Öztürk başkanlığında oluşturulan bir komisyon bir tasarı hazırlamıştı. Bu tasarı 2006 yılında Başbakanlığa gönderilmişti, Başbakanlık 2008 yılında bu tasarıyı Meclisimize sevk etmişti, Meclisimiz yine 2008 yılında esas komisyon olarak Adalet Komisyonunu belirledi, Adalet Komisyonu bir alt komisyon oluşturdu bu konuda teknik bir husus içermesi sebebiyle, ancak alt komisyon birkaç toplantıdan sonra konunun teknik olması, biraz ağır olması sebebiyle ve Meclis çalışmalarının yoğunluğu sebebiyle çalışmalarını devam ettiremedi, tamamlayamadı. Daha sonra seçimlerin yenilenmesi sebebiyle İç Tüzük’ün 77’nci maddesi uyarınca bu tasarı hükümsüz kaldı. Bunun üzerine, seçimlerin yenilenmesinden sonra Adalet Bakanlığı olarak 15 Eylül 2011 tarihinde Başbakanlığa tekrar yazı yazarak bu tasarinin yenilenmesini, Meclise sevk edilmesini talep ettik ancak tasarı henüz şu an Başbakanlıkta. Şu anki bulunduğu durum bundan ibaret ancak birtakım gelişmeler oldu bu arada, gerek Avrupa Birliği organlarında gerek mukayeseli hukuktaki birtakım düzenlemelerde gerek ülkemiz gerçekleriyle ilgili yapılan birtakım değerlendirmeler, daha önceki tasarıyla ilgili görüş ve öneriler dikkate alınarak biz Bakanlıkta bir çalışma grubu oluşturarak bu tasarinin güncellenmesine yönelik bir çalışma yürütüyoruz. Yakın bir zamanda sanıyorum

Başbakanlıkta bulunan resmî tasarı ile bizim hazırladığımız tasarı yeknesak hâle getirilerek Meclisimize sevk edileceğini öngörüyoruz.

Kişisel verilerle ilgili arzım bundan ibaret, “Ulusal Bilgi Güvenliği Kanunu”na geçmek gerekirse, günümüzde yine hepinizin malumu gerek kamu sektörü gerekse özel sektör tarafından sunulan çok sayıda hizmet zorunlu ve vazgeçilmez bir şekilde bilişim sistemleriyle yönetilmekte ve bunlar üzerinden sunulmaktadır. Hava yolları, barajlar, tren yolları, sinyalizasyon sistemleri, metrolar, bankalar, sigortacılık sistemi, sermaye piyasası, sağlık sektörü gibi pek çok alanda bilişim sistemleri yaygın bir şekilde kullanılıyor. Bu sistemlerin güvenliklerinin sağlanması da aynı derecede bu hizmetlerin verilmesi kalitesi kadar önemli bir husus. Bu sistemlere mukayeseli hukukta Avrupa ülkelerindeki yaptırmış olduğumuz çalışmalarda tasniflemeler yapılmış ve şu tür saldırıların olabileceği değerlendirilmiş. Öncelikle terör örgütleri tarafından bu tür sistemlere saldırılar olabilir, yine yabancı rakip veya düşman ülkeler tarafından bu tür bilişim sistemlerine saldırılar olabilir veya “hacker” diye tabir edilen meraklı gençler tarafından da bu tür saldırılar olabilir. Bu saldırıların kimden geldiğinin bir önemi yok, böyle bir saldırının kim tarafından ve hangi amaçla yapılmış olursa olsun bilişim sistemlerimizin bu tür saldırılara karşı, istismarlara karşı güvenliğinin sağlanması zorunluluğu söz konusu.

Ülkemizde önemli kurum ve kuruluşlar tarafından, istihbaratlarımız tarafından, güvenlik birikimlerimiz tarafından fiziki bir saldırı ihtimali baz alınarak çok ciddi çalışmalar yapılıyor, istihbarat üretiliyor ve güvenlik önlemleri artırılıyor ancak sanal bir saldırı olasılığına karşı yeterince hazırlık yapılması, bu konuda gereken önlemlerin alınması konusunda birtakım eksikliklerimiz var. Son on beş yılda pek çok Avrupa ülkesi bu konuda ciddi şekilde çalışmalar yaptılar, oluşturdukları siber güvenlik merkezleriyle 7 gün 24 saat üzerinden ülkelerindeki kritik altyapı sistemlerine, kamu kurumlarının sunmuş oldukları hizmetlere herhangi bir saldırı olup olmadığı, bunlara karşı ne gibi önlemler alınabileceği, krizlerin nasıl yönetileceği konusunda kafa yorup, stratejiler üretip, eylem planları hazırlayan birimler var. Bu konuyla ilgili Türkiye’de “E-Dönüşüm Türkiye Projesi” kapsamında bu konuya ağırlık verildi ve 2006-2010 yılını kapsayan Bilgi Toplumu Stratejisi ve buna ilişkin eylem planında Ulusal Bilgi Güvenliği Kanun Tasarısı’nın hazırlanması gündeme geldi ve bu görev Adalet Bakanlığına verildi. Yine, AB müktesebatının üstlenilmesine ilişkin metinlerde de bu konu gündeme alındı. Bu konuyla ilgili ilk defa da 2002 yılında Genelkurmay Başkanlığımızın bir çalışması olmuştu ancak bu tasarının içeriğindeki birtakım hükümler sebebiyle o dönem itibarıyla kabul görmedi ve bu tasarı Meclise sevk edilmedi. Ondan sonra Bakanlığımız bu görevi devraldı, 2009 yılında bir çalışma grubu oluşturdu ilgili kurum ve kuruluşların katılımıyla, bir taslak hazırlandı ancak 2010 yılındaki gerek Meclisin gerek Bakanlığın yoğun temposu içerisinde tali bir konumda kaldı ancak önümüzdeki günlerde, yakın bir gelecekte bu tasarıyla ilgili çalışmalar tamamlanıp en yakın sürede Meclisimize sevk edilecek.

Benim yüzeysel arzım bundan ibaret. Herhangi bir soru olursa elimizden geldiği kadar cevap vermeye çalışırız.

Saygılarımı sunuyorum efendim.

BAŞKAN – Çok teşekkür ediyoruz Sayın Taşkın.

Şimdi, Sayın Nurdan Okur, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürümüz, Siber Suçlar Sözleşmesi'yle ilgili çalışmalar hakkında bir sunum yapacak.

Buyurun efendim.

ADALET BAKANLIĞI ULUSLARARASI HUKUK VE DIŞ İLİŞKİLER GENEL MÜDÜRÜ DR. NURDAN OKUR – Sayın Başkanım, değerli milletvekilleri; ben Siber Suçlar Sözleşmesi'yle ilgili kısa bir girişten sonra özellikle çekinceler konusunda sözü Hâkimimize vereceğim.

Öncelikle şunu belirtmek istiyorum: 23 Kasım 2001'de beş yıl süren çalışmaların sonucunda Siber Suçlar Sözleşmesi Budapeşte'de imzaya açıldı, Temmuz 2004'te yürürlüğe girdi. Bu sözleşmeyi sadece Avrupa Birliği ülkeleri değil, sözleşmenin düzenlediği alanın küresel alana ilişkin olması sebebiyle dünyanın çeşitli ülkeleri imzaladı, Amerika'dan tutun da Kanada ve Güney Afrika'ya kadar. Yani bu sözleşmeyi toplam 47 ülke imzaladı ancak 33'ü onayladı, 14'ü henüz onaylamadı. Ayrıca Ocak 2012 itibarıyla 8 ülkeye daha imzaya açıldı. Bu ülkeleri Avustralya'dan Afrika'ya kadar, Latin Amerika'ya kadar dünyanın çeşitli ülkeleri yine 8 ülkenin içerisinde. Sözleşmenin imzalanmasından sonra en önemli argüman ülkelerin bu sözleşmeyle iç hukuklarını uyumlaştırması gerekiyor ve Siber Suçlar Sözleşmesi Avrupa Konseyinin 9 no.lu 89 sayılı Tavsiyesi'ne dayanılarak hazırlanmış olmasına rağmen daha ileri düzenlemeler dahi içermektedir.

Sözleşmeye baktığımızda sözleşme 46 maddeden oluşuyor. Amacına baktığımızda da iç hukukun sözleşmeye uygun hâle getirilmesi, uluslararası iş birliğinin bu suçlarla ilgili olarak geliştirilmesi, tüm taraf devletlerle benzer suç tipleri oluşturularak yeknesaklık sağlanması ve ortak bir ceza politikasının oluşturulması sözleşmenin amacı.

Sözleşme üç temel gövde üzerine kurulmuştur. Buna baktığımızda birincisi, yeni teknoloji kullanımıyla ilgili suçlara ait ortak tanımların oluşturulması. İkincisi, soruşturma yöntemlerinin tanımlanması. Üçüncüsü de, bizim görev alanımızı ilgilendiren daha çok, uluslararası iş birliğinin, buna ilişkin yöntemlerin sözleşmeyle geliştirilmesi.

Suç tiplerine baktığımızda belki suç tiplerini dört ana kategoride değerlendirmek mümkün. Bilgisayar veri sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına ilişkin suçlar birincisi. İkincisi, bilgisayarla ilişkili suçlar, sanal sahtecilik, sahtekârlık suçları bunların içinde söylenebilir. Üçüncüsü, içerikli ilgili suçlar. Örneğin, çocuk pornografisinde olduğu gibi. Dördüncüsü de fikrî mülkiyet haklarının ihlaliyle ilgili suçlar. Şimdi, sözleşmenin genel olarak düzenleme alanı bu, amacı da bu. Peki, bizim durumumuz ne? Biz 10 Kasım 2010'da sözleşmeyi imzaladık ancak henüz onaylamadık. Sözleşmenin onaylanması aşamasında birtakım çekincelerde bulunması gerektiğini düşünüyoruz ve Adalet Bakanlığı olarak da Dışişleri Bakanlığına bu çekincelerimizi belirttik.

Şimdi “Bu çekincelerimiz neler ve neden konulması gerekiyor?” hususunda hâkimimiz Mustafa Sabit Bey'e ben söz vermek istiyorum.

BAŞKAN – Çok teşekkür ediyorum Sayın Genel Müdürüm.

Buyurun Sayın Sabit.

ADALET BAKANLIĞI TETKİK HÂKİMİ MUSTAFA SABİT – Sunum planımızda zaten genel bilgileri ilk aşamada bahsetmek üzere göstermiştik, Genel Müdüre Hanım bir kısmı itibarıyla da zaten bahsetmiş oldu.

33 ülke tarafından hem imzalanıp hem onaylandı, 14 ülke de şu an imzalamış olup onaylamayı bekliyor, biz de artık onların arasındayız. Bahsedildiği üzere sözleşmenin yapısı maddi ve usul hukukuna ilişkin tanımlar ve bizim açımızdan da uluslararası iş birliğine ilişkin hükümler içeriyor. Genel olarak suçlar “şeklî suçlar” olarak sayılıyor. İçeriğe ilişkin, çocuk pornografisine ilişkin 9’uncu maddede düzenleme var. Ayrıca bunlardan ırkçılığa ilişkin hususlar ise ek protokolde düzenlenmiş olup isteyen ülkeler ayrıca ek protokole üye olmak suretiyle bunu da uygulama alanına sokabilecekler. İç hukukumuz bakımından henüz imzalayıp onaylamadığımız için bir bağlayıcılığı bulunmamaktadır, uluslararası hukuk açısından ise sözleşmeye taraf olursa dahi buna uyup uymama konusunda herhangi bir üst otorite bulunmamaktadır, tamamen uluslararası hukuk kurallarına göre ülkelerin karşılıklı mütekabiliyet ilkesi gereğince karşılıklı olarak uygulayacaklardır, herhangi bir mahkemenin yetkisi dâhilinde bulunmamaktadır.

Sözleşmede biçim açımızdan adli iş birliği hükümleri bulunduğu bahsetmiştim. Adli iş birliği hükümleri bu sözleşmeye ek olarak konulmuş hükümler, esasen Avrupa Konseyinde bizim “CİKAYAS” olarak kısalttığımız Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi bulunmaktadır. Bu adli yardımlaşmaya ilişkin temel hükümleri içeren bir sözleşmedir ve biz de zaten bunun tarafıyız. Avrupa Konseyindeki üye ülkelerin 46’sının 45’i de buna taraf. Bu sözleşme kapsamındaki adli yardımlaşmaya ilişkin temel bazı hükümler bu sözleşmeye, Siber Suçlar Sözleşmesi’ne de eklenmiştir çünkü Siber Suçlar Sözleşmesi’ne taraf olan ülkelerin bir kısmının “CİKAYAS” diye kısalttığımız sözleşmeye taraf olmama ihtimali bulunmaktadır. Nitekim de Siber Suçlar Sözleşmesi’ni Amerika, Japonya, Güney Afrika gibi ülkeler taraf olmuşlar ancak bunlar CİKAYAS’ın tarafları değildir.

Bu CİKAYAS, adli iş birliği alanında temel sözleşme olarak Siber Suçlar Sözleşmesi, bunu tamamlayıcı nitelikte bulunmaktadır. Hâlen bahsettiğim üzere Siber Suçlar Sözleşmesi’ni biz onaylayarak yürürlüğe sokmamış olmamıza rağmen bahsettiğim üzere CİKAYAS gereğince CİKAYAS bir temel sözleşme ve her türlü suça ilişkin adli yardımlaşma CİKAYAS’a göre yapılabilir. Mevcut olarak da biz bilişim suçlarına ilişkin adli yardımlaşmayı CİKAYAS ve ikili sözleşmelere, ikili sözleşmeye taraf olmadığımız ülkelere de mütekabiliyet kuralı gereğince yapmaya çalışıyoruz. Şu anda 450 ila 500 arasında bizden talep gitmektedir. Bu taleplerin çok büyük oranı da, yüzde 80 civarındaki bir miktarı da Amerika’ya muhataptır. Ne yazık ki bu taleplerimiz yine bir yüzde 80 oranında reddedilerek geri gönderilmektedir. Buradaki temel sebep de genellikle bizdeki suçlar “İnternet üzerinden işlenen suçlar” dediğimiz hakaret suçları ve bunlar, Amerika’da hakaret suç olarak kabul edilmediği için bu sebepten reddediliyor. Birtakım kredi kartı dolandırıcılıkları ise miktarın çok küçük olması nedeniyle reddediliyor.

Bahsettiğimiz üzere sözleşmede “şeklî suç” anlamında bilişim suçları düzenleniyor, içerik olarak sadece çocuk pornografisi var, ırkçılık ek protokolle düzenleniyor, terörizm konusu da yeni bir ek protokol konusu olarak düşünülüyor. Bu ırkçılık ve terörizmin ek protokol olarak düzenlenmesindeki temel felsefe de genel olarak sözleşmeyi herkes tarafından kabul edilebilir taraf olabilir bir nitelikli tutmak, böyle ırkçılık ve

terörizm gibi ülkeden ülkeye değişen hususları ek protokolde düzenleme ihtiyacından dolayı bunlar ek protokol konusu olmuşlardır.

Sözleşmede bahsettiğim üzere, CİKAYAS'ı atf eden suçluların iadesi, ifade alınması, bilgi, belge teminine ilişkin birtakım hükümler var, bunlar yeni hususlar değil, bu sözleşme bakımından adli iş birliği anlamındaki yenilik ise 7/24 irtibat ağı kurulması hususu. Bu esasen G 8 ülkelerinin yüksek teknoloji suçlarına ilişkin yaptıkları bir irtibat ağından örnek alınarak kurulmuş bir ağıdır.

Sözleşme içerisinde İnternet erişiminin engellenmesi veya engellenmemesine ilişkin herhangi bir hüküm bulunmamaktadır. Zaman zaman Avrupa Konseyinin çalışmalarında ülkelere yönelik tavsiye niteliğinde, engellenmemesi konusunda görüşler belirtilmekle birlikte bu henüz Avrupa Konseyi nezdinde de bir sözleşme konusu hâline gelmiş değildir.

Kişisel veriler, biraz önce bahsedildi, sözleşme kapsamında yine kişisel veriler açık olarak bahsedilmiyor ancak burada da karşılıklı talepler yapılıyor, bahsettiğim üzere adli yardımlaşma hükümleri var, özellikle 7/24 irtibat ağı üzerinden birtakım kişisel verilerin talep edilmesi durumuyla karşılaşacağız. Dolayısıyla da kişisel veriler kanunu olmadığı için bu alınan ve verilen, karşı taraftan talep edilecek verilerin neler olabileceği konusunda mevzuatımızda şu an bir boşluk bulunmaktadır, dolayısıyla da bu uygulayıcının takdirine kalabilecektir veya sakıncalı olabilecektir. Bu yüzden de kişisel veriler kanununun da kanunlaşması bu anlamda, bu sözleşme, özellikle 7/24 irtibat ağının çalışması açısından önem arz etmektedir.

Sözleşmeye taraf olmak, bahsettiğim üzere, biz bu sözleşme olmasa da CİKAYAS gereği bilişim suçlarına ilişkin adli yardımlaşmayı yapabiliyoruz ancak sözleşmeye taraf olmak bir imaj meselesi hâline gelmiş bulunmaktadır uluslararası arenada, özellikle de bu kişisel verilerin korunmasına ilişkin kanun için de bu çok geçerli bir husus. Bizim, Amerika'dan yaptığımız taleplerin bir kısım itibarıyla reddedilmesinde bizim bu sözleşmeye taraf olmamamızın da etkisi olduğunu düşünmekteyiz. Nitekim ülkeler bu sözleşmeye taraf olmayan ülkelere karşı bir ön yargı içerisinde bakmaktadır. Şimdi ismini zikredemeyeceğim bir kısım ülkeler de bu siber suçlar odaklanmış hâlde ve örgütlü olarak yapılmaktadır. Dolayısıyla da bu sözleşmeyi imzalamayan ve onaylamayan ülkeler o ülkeyle birlikte aynı kategoride değerlendirilebilmektedir.

Dört-beş yıldır bu sözleşmeye taraf olması konusunda İçişleri Bakanlığı, Dışişleri Bakanlığı, Ulaştırma Bakanlığı, Kültür Bakanlığı ile birlikte mevzuatımızın değerlendirilmesi çalışmaları yapılıyor. Bu yapılan çalışmalar sonucunda mevzuatımızın bu sözleşmeye yüzde 90'ın üzerinde bir şekilde zaten uyumlu olduğu yani o sözleşmede getirilen, öngörülen suçlar zaten bizim mevzuatımızda suç olarak mevcut. Çok kısmi denecek sözleşmenin birkaç maddesinde çekince koymamızı gerektirecek hususlar var. Bunlara ilişkin Türk Ceza Kanunu'ndaki "doğrudan bilişim suçları" dediğimiz suçları burada görüyoruz. Ayrıca bilişim sistemleri üzerinden işlenen birtakım suçlar var. Yine bazı özel kanunlarda bu konuya ilişkin düzenlemeler var. Bu düzenlemeler kapsamında yapılan analiz çalışmaları sonucunda işte yine bahsettiğimiz kuruluşlar burada gösteriliyor.

Sözleşmenin 42'nci maddesi hangi maddelere çekince konulabileceğini bahsediyor. Bunlar ekranda görülüyorlar. Bu çekince konulabilecek maddelerden 4'üncü maddeye herhangi bir çekince konulmasına karar verilmiştir. 6'ncı maddede cihazların kötüye kullanılması mevzuunda Siber Suçlar Sözleşmesi'nde "satımı,

dağıtımı ve ithali” gibi bir ifade var, bizim mevzuatımızda “ithal” ifadesi yoktu, ancak Kültür ve Turizm Bakanlığı 5846 sayılı Yasa’da bir değişiklik öngörüldüğünü ve bu değişiklikle bizim mevzuatımızın da tamamen uyumlu olacağına kanaat getirdiği için orada da bir çekince konulmasına gerek olmadığı... 7’nci maddede sahtecilik fiilleri düzenleniyor. Bizim mevzuatımızda “resmî belgede sahtecilik” ve “özel evrakta sahtecilik” diye iki ayrım var. Özel evrakın kasıtlı olarak bir dolandırma, sahte evrak düzenleme kastı ve onunla bir şekilde menfaat elde etme kastı olması gerektiği için bu hususun çekince olarak belirtilmesinin uygun olduğu kanaati uyanmıştır ve bu şekilde bildirilmesi düşünülmektedir.

Çocuk pornografisine ilişkin olarak çok büyük oranda sözleşmedeki hükümleri 5651 sayılı Yasa karşılamaktadır. Bu yüzden o mevzuda da bir çekince konulmasına gerek görülmemiştir. 10’uncu madde konusunda henüz bir karara varılmamıştır. Kültür Bakanlığı henüz bu konuyu değerlendirmektedir. 11’inci maddede bir çekince konulmasına gerek yoktur. 22’nci madde ise yargı yetkisine ilişkin bir husustur. 22’nci maddede genel olarak bilişim suçlarını bir vatandaşımızın işlemesi hâlinde, yurt dışında dahi işlese Türkiye’de bulunduğu takdirde yargılanmasına yönelik bir düzenleme bulunmaktadır. Türk Ceza Kanunu’nun 11’inci maddesi de aynı hususu düzenlemektedir ancak Türk Ceza Kanunu’nda da bir sınırlama var, o da suçun bir yılın üzerinde bir hürriyeti bağlayıcı cezayı gerektirdiği husustur. Siber Suçlar Sözleşmesi böyle bir yıllık cezayı gözetmediği için biz bu açıdan 11’inci maddeye uygun olarak bu 22’nci maddeyi uygulayacağımız konusunda bir çekince belirtmeyi uygun görmüştük.

29’uncu maddede gelecek taleplerin... Diyelim ki başka bir ülke siber suçlar konusunu daha geniş düzenlemiş ve bizde suç olmayan bir hususu da siber suç olarak değerlendirmiş olabilir. Biz bu açıdan çifte cezalandırılabilirlik kuralı gereğince bu talepleri yerine getireceğimize dair bir çekince bildirilmesinin uygun olacağını değerlendirmekteyiz.

Son olarak 24’üncü ve 27’nci maddeler ise çekince değil, bunlar bildirim ve bahsettiğim üzere “Uluslararası adli iş birliğinde merkezi makam kim olacak?” hususu. Türkiye’de bütün adli yardımlaşma konularında merkezî makam Adalet Bakanlığı. Bu nedenle bu konuda da görüş birliğine varılmıştır ancak 35’inci madde yani 7/24 irtibat ağının hangi bakanlık nezdinde kurulacağı konusunda Adalet Bakanlığı ve İçişleri Bakanlığı arasında görüş birliğine varılamamıştır. Bizim düşüncemiz 24’üncü ve 27’nci madde gereğince normal yoldan yapılacak adli iş birliğinin bir kısım parçalarının 7/24 üzerinden yapılması ve bizim hiçbir haberimiz olmadan buradan geçmesi söz konusu olabileceğinden ve bir adli yardımlaşma politikasının bu şekilde bütüncül olarak yürütülemeyeceği düşünüldüğünden öncelikle Adalet Bakanlığı bu konuda düşünülmelidir, olmadığı takdirde de Adalet Bakanlığı denetiminde İçişleri Bakanlığına da bu şekilde görev verilebilir çünkü 7/24 irtibat ağına hem adli iş birliği, adli yardımlaşma talepleri hem de polisiye iş birliği kapsamında talepler gelebilecektir. Dolayısıyla da Adalet Bakanlığı adli iş birliğine ilişkin taleplerde şu an merkezî makam olarak tek yetkilidir, dolayısıyla da bu konuda da bu hususun göz önünde bulundurulmasını biz yaptığımız görüşmelerde dile getirmiştik.

Teşekkür ediyorum.

BAŞKAN – Çok teşekkür ediyoruz.

UYAP sunumunu kim yapacak arkadaşlar? Mesut Orta mı?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Evet efendim.

Sayın Başkanım, sayın milletvekilleri; öncelikle hepinizi saygıyla selamlıyorum.

Bu sunum kapsamında UYAP Bilişim Sistemi hakkında bilgiler vermeye çalışacağım, ardından da bilişim sistemleriyle ilgili böyle bir sistemi yönetirken, işletirken ve kurma aşamasında karşılaştığımız, diğer kurumlara da örnek olabilecek birtakım önerilerimiz en sonunda olacaktır.

Öncelikle çok kısa bir şekilde UYAP nedir? Önce isminden başlamak istiyorum, Ulusal Yargı Projesi'nin, daha sonradan biz bunu bir marka hakkı alarak UYAP olarak isimlendirdik. Amacımız da projeye başladığımızda sadece ilk derece mahkemeleri değil, yüksek yargıyı da içine kapsayan, belki kolluk kuvvetlerini de içine alan süreç bazlı bir bilişim sistemi oluşturmaktır. Bu nedenle sadece başka bir isim verilebilirdi ama tamamını kapsayacak şekilde UYAP ismi verildi. Proje, baştan sona kendi öz kaynaklarımızla, kendi mühendislerimizle gerçekleştirildi, herhangi bir fon kullanılmadı. Buradaki bu bilişim sistemini kurarken yola çıktığımızda ilk hedefimiz şuydu: Kâğıtsız ofis ortamını gerçekleştirmek.

HAYDAR AKAR (Kocaeli) – Sayın Başkan, UYAP'ın içerisinde bizim Komisyonun amacına yönelik bir bilgi var mı şu anda, onu versinler bize.

BAŞKAN – Ben detayını bilmiyorum yani isterseniz o şekilde sorarım, o şekilde anlatsınlar kısaca.

HAYDAR AKAR (Kocaeli) – O zaman bütün konuları, yaptıkları uygulamaları dinlemek durumumda kalırız, amacımız bu değil.

BAŞKAN – Tabii.

Peki, Bilişim ve İnternet Komisyonu ile ilgili yani bu bilişim suçlarıyla mücadele anlamında bir yönü var mı Sayın Daire Başkanı?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Efendim, benim kanaatim, doğrudan ilgili olduğunu düşünüyorum çünkü “bilişim suçları” dediğimiz suçlar genelde bu bilişim sistemleri üzerinde işlenmekte ve büyük oranda da kamu kurumlarının bilişim sistemlerindeki açıklıklar, zaafılar kullanılarak yerine getirilmektedir. Yani o anlamda...

HAYDAR AKAR (Kocaeli) – UYAP'ın veya Adalet Bakanlığının bilişimdeki açıklarını, varsa, eğer avantajlı tarafları varsa diğer kurumlara olduğu gibi onları anlatın. Yani UYAP'ın savcı ve hâkimlere sağladığı ya da mahkemelere getirdiği kolaylıkları istemiyoruz, öyle bir beklentimiz yok sizden. UYAP Projesi'nde işte hâkimin, savcının ulaşabildiği, avukatın ulaşabildiği, dosyaya ulaşabildiği şeyleri istemiyoruz sizden, yani sizin bu sistemi kurarken karşılaştığınız sıkıntılar, örneğin, biraz evvel söylediğiniz ya da bu sistemi kurduktan sonra farkındalık yaratarak diğer kamu kuruluşlarından öğreneceğiniz, işte siber suçlar veya bir hacker tarafından “hac” edilme olayını önleyebilmek için neler yaptınız? Eğer varsa bunları anlatın.

BAŞKAN – Yani dosya birikimini filan engelleyerek hâkim ve savcıya yardımcı oluyorsa o sonuçta yargı sistemine de yardımcı oluyordur yani Sayın Akar.

HAYDAR AKAR (Kocaeli) – Yani anlatmasınlar diye söylemiyorum, ben bu şeyi ötelemek için de söylemiyorum, yani tamam güzel şeyler vardır, mutlaka...

BAŞKAN – Oraya odaklanarak anlatırsak Sayın Orta.

Evet, buyurun.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Tabii ki.

Şimdi, bu bilişim sistemlerinin özellikle bence üzerinde durulması gereken kısmı entegrasyonlar çünkü bilişim sistemleri kendi başına bir şey ifade etmezler. Evimizdeki İnternet'e bağlanmayan bir bilgisayar gibi ki uluslararası arenada İnternet'e bağlı olmayan bilgisayarları bilişim kullanıcısı olarak da kabul etmiyor şu anda dünya. O anlamda bir sistemi ele aldığımızda diğer sistemlerle bağlantılarına da bakmak gerekir. Örneğin bizim sistemimizde şu anda hem avukatların hem vatandaşların doğrudan hizmet alabildiği, bu aynı zamanda açıkların olabileceği muhtemel yerler demektir.

Yine, “bilişim” terimi kapsamında ben özellikle kamudaki yapılanma çünkü yapılanmayla çok doğrudan ilgili bir şey, bir kamu kurumunda eğer aynı bakanlık içerisinde altı tane bilgi işlem daire başkanlığı varsa, bu projeler birbirleriyle konuşmıyorsa, bunların güvenliği konusunda ortak bir konsept geliştirilememişse bu sonuç olarak bize bilişim suçları olarak dönmektedir.

Amaçları geçiyorum. Ancak burada UYAP'ın amaçlarından bir tanesi şu: Biz şu anda 60 bin kullanıcıya hizmet veriyoruz, iç kullanıcıya. Bir şekilde bunlar İnternet'e çıkıyorlar, bir şekilde tabii ki avukatlar olsun, vatandaşlar olsun bu sisteme dışarıdan erişebiliyor. Sistemi ilk kurup hayata geçirdiğimiz 2004 yılında bir yönetmelik çıkardık. Bu yönetmelik Resmî Gazete'de yayımlanmadı, Başbakanlığımız uygun görmedi ancak burada her bir kullanıcının nelere uyması gerektiği, ne yapması gerektiği konusunda bir farkındalık oluşturmak istedik. Hatta daha sonra yaptığımız bir araştırmada kullanıcılara ilk verdiğimiz şifrenin bir yıl sonra bile değiştirilmediğini, genellikle çocuklarının isimleri, doğum tarihleri ya da sicilleri gibi birtakım şeylere bağlandığını gördük. Bunları çözmek için de kendi içimizde kırk beş günde bir zorunlu hâle getirdiğimiz daha önceki şifreyi kabul etmeyen bir mekanizma geliştirdik ve bu yolla herkes şu anda kırk beş günde bir yeni şifre kullanmak zorunda.

Bir başka yönüne de değinmek istiyorum, o da şu: Bilişim sistemleri hem donanım hem de yazılım itibarıyla genelde yurt dışı kaynaklı şeylerden oluşmaktadır, dolayısıyla içeriğini bilemediğimiz kodların, örneğin bir windows işletim sisteminin hangi bilgileri dışarıya gönderdiği konusunda emin olmak mümkün değildir. Bu nedenle yerli yazılımın ve yerli donanımın kullanılması önem arz ediyor. UYAP üç tane katmandan oluşuyor. Bunlardan bir tanesi editör, ikincisi doküman yönetim sistemi, üçüncüsü de yargı teşkilatının kullandığı uygulamalar. Bunların tamamı kendi mühendislerimizce “açık kaynak kod” diyebileceğimiz, kodları kendi elimizde olan, lisans hakları kendi elimizde olan bir şekilde gerçekleştirilmiştir. Bilişim suçlarına bakan yönüyle bu çok dikkate değer diye düşünüyorum.

Bir diğeri de şu anda uygulama sadece ilk derece mahkemelerini değil, yüksek yargının tamamını da kapsamaktadır. Az önce bahsettiğim, gerek yerli olması gerekse tek bir elden yönetilmesi, tek bir elden korunması, bunun için gerekli insan kaynağının sağlanması açısından da “Bulut bilişim” diye son dönemde çok fazla konuşulan kavram Adalet Bakanlığında, yargı teşkilatında şu anda hayata geçirilmiş durumdadır. Kolluk kuvvetleriyle bir çalışma başlatılmıştır, Jandarma Genel Komutanlığı şu anda kullanmaya başlamıştır. Adli işlemlerle ilgili her türlü bilgi, belge tek bir sistem üzerinden aktarılmakta, tek bir sistem üzerinden gerekli güvenlik kontrolleri yapılmaktadır.

Bizim biliřim sistemine baktığımızda özellikle yine önem arz eden bir konu da acil durum merkezleridir. řu yönüyle önem arz ediyor: Bu sistemlerin fiziksel saldırıya uğraması durumunda ya da hack'lenmesi durumunda bir řekilde bu sistemlerin durmadan yoluna devam etmesi önemlidir çünkü sisteminiz durduğunda o hizmeti veremezsiniz. Bu anlamda bizim yine kendi bire bir sistem merkezimizle aynı olan, aynı řekilde korunan, aynı řekilde güvenlik tedbirleri alınan, yamaları yapılan ikinci bir biliřim sistemimiz bulunmaktadır. Bu da önemli bir husus diye düşünüyorum.

Bu sistemlere farklı bir gözle de baktığımızda řu anda mobil dünyaya kayış var, mobil dünyaya doğru gidiliyor, dolayısıyla her türlü uygulamanın mobili yapıyor ve insanların mobil cihazlardan bunlara erişiminde de yine bir bilinçlendirme hareketinin yapılması gerekiyor. Örneğin, řu anki cep telefonları bir fotoğraf çektiğinizde bulunduğunuz yer bilgisini, konum bilgisini fotoğrafın içerisine gömmekte, o yere tekrar gitmek istediğinizde o fotoğrafa dokunmanız durumunda aynı yere gidebilme tesiniz.

Vurgulamak istediğim bir yönü de řu: Biz projeye başladığımızda řunu yapabiliirdik: Bütün hâkim, savcılara bilgisayar verirdik, mahkemelere bilgisayar verirdik ve onlar bir řekilde word üzerinden bu işlemleri yapabiliirdiler ancak bu bir biliřim sistemi olmazdı, hem onların okuryazarlığını artırma hem de kontrolünüzde olan nerede ne cereyan ediyor bilebildiğiniz bir sistemi oluşturmak adına sistemin tamamını baştan sona ele almak da biliřim güvenliği açısından da ayrı bir önem arz ediyor.

Bütün fonksiyonel yapı UYAP'ın içerisinde. Bu řu demektir, işin bir taraftan da vahametini söylüyor aslında: řu anda kâğıt üzerinde yapılan, UYAP harici yapılan herhangi bir işlem bulunmamaktadır. Bütün işlemlerin tamamı, sayı, tarih, numara alma, yazı yazma, bunların tamamı UYAP üzerinden gerçekleşmektedir. 57 kurum sistemiyle řu anda veri alışveriři sağlamaktayız. Burada biliřim güvenliği açısından řu noktaya dikkatinizi çekmek istiyorum: Dış kurumlarla yapılan veri alışverişinde bir kurum verilerini diğer kuruma açmış demektir. Bu konuda gerekli protokoller uygulanmazsa bu entegrasyonlar biliřim sistemlerinin büyük bir açığı olarak değerlendirilebilir. Biz kendi bünyemizde bu amaçla bir veri değerlendirme komisyonu kurduk, hangi veriler hangi kurumlara verilmeli, hangi veriler diğer kurumlardan alınmalı, bununla ilgili ayrı bir komisyon oluşturuldu.

Bu kısmı geçiyorum. řu açıdan önemli olabilir: Mahkemenin önüne biliřim suçu geldiğinde başka bir sisteme girme, oradan bir yetkisiz erişim söz konusuysa bu sistemlerde kim nereden, hangi makineden hangi tarih ve saatte hangi sorgulamayı yapmış, bunların log kayıtları tutulmaktadır. řu anda da bize başsavcılıklardan bu řekliyle yazılar gelmektedir. Bu yazı geldiğinde biz IP'sini, web adresini, vesaire, hepsini verip bu sorgulamanın nerede yapıldığını anlık olarak söyleyebilmekteyiz.

Aynı řekilde yine Komisyonun dikkatini çekebilecek bir husus, biliřim sistemlerinde yetkilendirme, kimin nereye eriştiği, hangi bilgisayardan hangi IP'lere kullanıcı adıyla eriştiği biliřim suçlarıyla ilgili yapılacak soruşturmada büyük önem arz ediyor. Çünkü örneğin wireless'ı olan bir otobüsün yanından geçen bir arabadan yapacağınız bağlantıyla işleyeceğiniz herhangi bir biliřim suçunu asla çözemezsiniz çünkü onun kim olduğunu bulma şansımız yok. Burada da aynı řekilde, 60 bin kullanıcı bir sistemde bunları tutmazsanız,

bunları takip edemezseniz, biliřim suçlarıyla ilgili pek çok dosyanız açık kalır.

Bunlar, şu anda entegrasyon sağladığımız yirmi yedi kurumun isimleri. Bunlardan bir iki tane örnek vereceğim. Bunu geçiyorum.

BAŞKAN – Bence hızlı geçin, son önerilerinizi alalım Sayın Orta.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Tamam efendim.

Elektronik imza her yerde kullanılıyor.

Şu dikkatimizi çekebilir: Şu anda araçlar üzerine tedbir kayıtları on-line koyulmaktadır. Dolayısıyla, bir mahkeme veya icra dairesi yazı yazmak yerine doğrudan sistem üzerinden gerekli takyidat şerhini koyabilmektedir.

Karar desteği geçiyorum.

Bu verdiğimiz hizmetleri de geçeceğim.

BAŞKAN – Önerilerinizi alalım Sayın Orta.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Peki.

Önerilerimizden birincisi, aynı kurumda birden fazla bilişim birimi bulunmaması gerekir çünkü bu bilişim sistemleri daha sonra birbiriyle veri alışverişi yapamamaktadır, yönetimi zor olmaktadır. Bu nedenle, kurum bazında tek bir bilişim sisteminin bulunması ve buna gerekli yatırımın yapılması hayati önem arz ediyor.

Rekabetçi ve yeterli bilişim ağı altyapıları sağlanmalıdır. Ağ altyapınız yeterli değilse ya da gerekli güvenliği sağlamıyorsa burada da çok fazla ihlaller olabilecektir. Bu anlamda network altyapısının güvenli olması çok önemli. Kurumlar şu anda bilgilerini network'e teslim etmekte, karşı tarafta da almaktadır. Dolayısıyla, yolda giderken yapılacak olan müdahaleler veya izlemeler önlenmelidir.

Yine bizim zorlandığımız konulardan birisi, bakım anlaşmaları ya da lisans alımlarında, müstakil yapıldığı için bunlar, bire bir kalmaktayız firmalarla. Bu, devlet adına tek elden yapılsa ya da çerçevesi belirlense, zannediyorum bu konuda da devletimizin çok büyük bir tasarrufu olacaktır, firmalarla yapılacak anlaşmalarda daha güçlü olarak karşılarına çıkmak mümkün olacaktır.

Kurumlar arası entegrasyonlarda her kurum şu anda diğer kurumla oturup “Bu bilgiyi bana verirsin, vermezsın.” kavgası yapmaktadır çünkü her kurumla protokol yapmanız gerekiyor. Buna ikna etmek, o süreçleri geçmek çok zor olmakta. O nedenle, e-Devlet kapısı baştan böyle yapılandırılmıştı ama e-Devlet kapısının bu fonksiyonunun bir an önce aktif edilmesi gerekiyor. Her kurum bire bir bağlantı yapmaya çalışıyor.

Bir diğer önerimiz, bilişim personeli politikası gözden geçirilmeli. Özellikle 657’de 4/B’de çözümleyicilerde yüzde 25 artı bir ücret veriyoruz şu anda fakat aynı işi yapan “mühendis” sıfatındaki diğer personele biz bunu vermediğimizde sıkıntılar oluşmaktadır.

Ve yine çok güzel bir düzenleme, 375 sayılı; 4 kata kadar bilişim uzmanı çalıştırma imkânı getirildi ancak burada, 5 bin ve daha üstü hizmet veren kurumlara 30 kişilik bir kontenjan tanındı. Biz 60 bin kişiye hizmet veriyoruz. Kurum olarak da altı-yedi tane büyük yargı teşkilatına hizmet vermemize rağmen 30 rakamı ile sınırlıyız. Bir ölçeklendirme yapılmamıştır burada. Bir ölçeklendirme yapılması çok faydalı olacaktır.

Ve yine bilişim sistemlerinin gerek geliştirilmesi gerekse iyileştirilmesi konusunda ceza sisteminin yanında bir de ödüllendirme mekanizması faydalı olacaktır diyoruz. Türkiye son dönemde çok güzel kamu

bilişim projeleri gerçekleştirdi fakat yurt dışında bunların etkin tanıtımı yapılamadı. Bunlar tanıtılırsa bu konuda Türkiye'nin ne kadar mesafe katettiği görülecektir.

Ve yine şu an UYAP için gündeme gelen projelerin ihracat altyapısının oluşturulması da ihtiyaçlarımızdan birisidir.

Güvenlik açısından elektronik imza mutlaka teşvik edilmeli çünkü güvenliğin en önemli unsurlarından birisi. Belçika diye hatırlıyorum, elektronik imza alan her vatandaşının yüzde 65 oranında elektronik imza ücretini karşılıyor. Bu şekilde bir yönlendirme olabilir.

Yine, kamuda ortak ihtiyaçlar için mükerrer yatırımlar yapılıyor. Bu yapıldığında güvenlik tam dikkate alınamayabiliyor, prosedürlere çok uyulamayabiliyor. Örnek vermek gerekirse, kamuda bir tane doküman yönetim sistemi olsa, bunun güvenliği, izlenmesi, her şeyi test edildikten sonra bütün kamuda kullanılıyor olsa, zannediyorum daha az problemle karşılaşırız.

Son maddem, bütün bunları gerçekleştirecek, takip edecek bir üstyapı oluşturulmalıdır. Yapının adı bakanlık mı olur, müsteşarlık mı olur, o ileride belki takdir edilebilir ama bu konuda bu problemleri sahiplenecek bir kuruma ihtiyaç olduğunu düşünüyorum.

Saygılarımla.

BAŞKAN – Çok teşekkür ediyorum.

Sayın Atıcı...

AYTUĞ ATICI (Mersin) – Teşekkür ederim Sayın Başkan.

Daha önce de bizim Komisyonumuzda bir konuyu gündeme getirmiştik, şimdi Adalet Bakanlığından bu kadar yetkililer buradayken tekrar gündeme getirmek istiyorum.

Yargıtay Cumhuriyet Başsavcılığının sitesine nüfus cüzdanınızın seri numarası ve T.C. kimlik numaralarınızla girdiğinizde hangi partiye üye olduğunuz çıkıyor. Bunun sakıncalarını içeren bir soru önergesini vermiştim zaten, sanıyorum Adalet Bakanı onu dikkate alacaktır. İşe girişlerde, şurada, burada kullanılan bir prosedür hâline gelmiş. Bu UYAP'ın bir ürünü müdür, bundan bilginiz var mı, böyle bir uygulamayı nasıl buluyorsunuz?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Bildiğim kadarıyla UYAP harici bir uygulamadır. Yargıtay Cumhuriyet Başsavcılığının siyasal partilerle ilgili ayrı bir birimi var, onların geliştirdiği fakat iletişim altyapısında da UYAP'ı kullandıklarını biliyorum. Çok fazla detay bilgiye sahip değilim ama notlarımızı alıp tekrar bakabiliriz.

AYTUĞ ATICI (Mersin) – Peki.

Eğer daha sonra bilgi verirsiniz sevinirim çünkü bu, gerçekten olağanüstü bir şey, gerçekten son derece tehlikeli bir şey. Pervasızca kullanılıyor; insanlardan işe girişte nüfus cüzdanı örneği alınıyor ve herhangi bir partiye üye olup olmadığını oradan, herhangi bir kimse tarafından, siz, ben, hepimiz o siteyi kullanarak sorgulayabiliyoruz. Örneğin, Cumhuriyet Halk Partisine kayıtlı iseniz işe alınmıyorsunuz veya tam tersi, işe alınıyorsunuz gibi. Hangi parti olursa olsun son derece suistimale açık bir şeydir. Yani bunu siz, yargıçlar veyahut da Adalet Bakanlığı yetkileri kendi aranızdaki sohbetlerde de konuşabilirsiniz. Yani bunun bir şekilde önüne geçilmesi lazım.

HAYDAR AKAR (Kocaeli) – Sunum için teşekkürler.

Aslında son kısımda, öneriler kısmında gerçek şeyleri söylemeye başladınız. İlk kısımlar çok ilgilendirmiyordu bizi ama burada koymuş olduğunuz teşhisleri çok yerinde ve iyi teşhisler olarak düşünüyorum. Örneğin, aynı kurumda birden fazla bilişim kurulunun bulunmaması, bana göre doğru bir olay. Niye doğru? Çünkü aynı ihtiyaçlar, aynı kurumlar tarafından tekrarlanarak yapılıyor.

İki: Güvenlik anlamında baktığınız zaman zaafılar doğuruyor. Bir kurumun işletim sistemi farklı, diğer kurumun işletim sistemi farklı olabiliyor, yine kullandıkları software'ler farklı olabiliyor. Bunların hepsi doğru.

Aslında burada yapılması gereken şey, sizin de az buçuk önerilerinizde belirttiğiniz, bir laboratuvar - bu TÜBİTAK'ın denetiminde olabilir veya bunun dışında olabilir- sistemi gibi yani devletin, kamunun kullanacağı -önce hardware'lerden başlayalım- hardware'ler sertifikalandırılmalı. Yani adalet dairesinde kullanılacak PC'yle Gümrük Bakanlığında kullanılacak PC'nin ve Ticaret Bakanlığında, Ekonomi Bakanlığında, kurumlarında kullanılacak PC'nin certified özelliklerinin aynı olması lazım, bir.

Ve bunların tümünün işletim sistemleri tek bir noktadan sisteme takıldığında yüklenmeli, iki, bu certified sistem sonucunda.

Ve bu kurumlarda hangi kurumların hangi software'leri kullanacağı tanımlanmalı, üç. Eğer gerçekten güvenli bir İnternet ve güvenli bir bilişim altyapısı kurmak istiyorsak bunlar yapılmalı.

Yine, bütün kurumların kullandığı işletim sistemleri özellikle... İşte, ne kullanıyoruz? XP vardı, en son Windows 7'ye mi geçtik? Şimdi kurumlar gelişigüzel bunları kullanıyorlar, daha sonra Outlook çıkıyor. Outlook versiyonu değişiyor, bunların yetmediğini görüyoruz. Şimdi ne yapıyor? Bir kurum Outlook'u değiştiriyor, diğer kurum XP server'ini değiştiriyor, diğer bir kurum PC'sini değiştiriyor ve bir entegrasyon yok, bir standardizasyon yok. Bunun da önüne geçebilmenin tek şartı, dediğimiz gibi, bir ortak kurum oluşturmak. Biz hep Erdal Bey'le bilişim bakanlığından bahsediyoruz. Bir bilişim bakanlığı çatısı altında kurumların yapılandırılması ve kullanacakları hardware ve software'lerin tanımlanması.

Sizin lisans alımlarıyla ilgili şeyinize katılıyorum. Bütün kurumlarda Microsoft'un ofis programları kullanılıyor ama her kurum kendisi alıyor bunu. Bazı kurumlar Devlet İhale Kanunu'yla alıyor, bazı kurumlar da serbest atışla alıyor, artık yöntemini söylemeyeyim ama...

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Bakanlığımızda yok, kullanılmıyor.

(Oturma Başkanlığına Kâtip Üye İzmir Milletvekili Erdal Aksünger geçti)

HAYDAR AKAR (Kocaeli) – Yok, hiç kullanılmıyorsunuz.

Ama bir ihtiyaçtır, kullanılmalı mıdır? Kullanılmalıdır ama şu yapılmalı: Sizin Bakanlıkla ilgili konuşmuyorum yani Türkiye'deki bilişimdeki, kamu kurumlarındaki bilişimdeki zaafılarımızla ilgili konuşuyorum.

Siz 60 bin kişisiniz; tüm kamu kurum ve kuruluşlarının kullandığını düşündüğümüzde belki Microsoft'u kullanan 500 bin tane -kullanıcı demeyeyim de- bilgisayar var, desktop var ve bunların her biri satın alınarak, lisanslanarak birçoğu da kaçak yüklenerek ama siz Microsoft'la bunun bir lisans anlaşmasını yaparsanız -devlet olarak ve kurumlarda kullanacağız- bu maliyetler çok aşağıya çekilecektir ve bir standart...

BAŞKAN – Sayın Vekilim, Microsoft’ tan çıkalım mı?

HAYDAR AKAR (Kocaeli) – Çıkalım, tamam, örnek olarak veriyoruz.

BAŞKAN – Beraber konuştuğumuz şekilde devam edelim seninle.

HAYDAR AKAR (Kocaeli) – Şeyden, nasıl diyelim onu...

Peki, devam ediyorum. Yine güvenlik. Dediniz ki: “Biz işte birden fazla –birden fazla demeyeyim de- aynı sistemin bir yedeğini de tutuyoruz.” Nerede tutuyorsunuz bunu örneğin, yedeğini?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA -Gölbaşı’ndan sonra 20 kilometre açıktaki...

HAYDAR AKAR (Kocaeli) – Farklı bir lokasyonda tutuyorsunuz.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Evet, ayrı bir lokasyonda.

HAYDAR AKAR (Kocaeli) – Doğru olan da bu. Ama her iki sistemi de aynı şekilde idame ettirmek durumundasınız. Sonuçta Network ağlarıyla bunu birbirine bağlıyorsunuz. Bunun yanında, tabii bunların sizin için ne kadar önem arz ettiğine bağlı olayın, ki çok önemli bir şey. Bir başka kurum için bunu yapmıyordur, diğer bir kurum farklı davranıyordur.

İşte, demek istediğim şu: Bilişim bakanlığı altında veya bilişim kurumu altında bütün kamu sektörünün... Aslında son önerilerinizi kamu kurum, kuruluşlarına doğru kanalize edebiliriz yani daha genelleştirebiliriz, o öneriler doğru önerilerdi, hep burada dillendirdiğimiz öneriler.

Söyleyeceklerim bunlar. Yani ben çok şey olmadığım için yani savcı, hâkim veya yargıdan olmadığım için sizin oradaki software’lerinizi veya geliştirdiğiniz programları çok merak etmiyorum ama tabii altyapısı önemli sistemin.

Bir şey daha soracağım. Bu 60 bin tane sizin kullanıcınız var, artı avukatlar da sisteminize bağlanıyor. Değil mi?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Doğru.

HAYDAR AKAR (Kocaeli) – Bu 60 bin kullanıcı aynı kanaldan mı İnternet’e çıkıyor, sizin üzerinizden mi çıkıyor İnternet’e yoksa her biri kendi, örneğin -ben Kocaeli Milletvekili olduğum için soruyorum- Kocaeli adalet dairesindeki sistem, kendisinin oradaki bir Telekom’la yapmış olduğu bir anlaşmayla mı İnternet’e çıkıyor? Eğer sizin üzerinizden çıkabiliyorsa denetlenmesi veya risklere karşı önlem alınması daha kolay ama oradan bağımsız çıkıyorsa sizi de riske sokma olasılığı daha yüksek.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Tek merkezden çıkıyor, 1.200 tane lokasyonumuz var, cezaevi, Adli Tıp Kurumu, vesaire gibi. 1.200 noktayı biz tek bir yerde topluyoruz, merkezde ve bunun önünde firewire’larımız var, IDS, IPS’lerimiz var, bu saldırı önleme ve saldırı...

HAYDAR AKAR (Kocaeli) – Avukatlar da buna dâhil mi?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Avukatlar farklı bir kanaldan geliyor, “DMZ” dediğimiz yarı güvenli bir bölgeden. Onlar dışarıdan hizmet alıyor.

BAŞKAN – Avukatlarda elektronik imza var mı?

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Mecburi efendim.

BAŞKAN – Yani ellerinde var.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Elektronik imza olmadan biz kimlik doğrulamasını kabul etmiyoruz, her girişlerinde elektronik imzayla bir belge imzalıyorlar, ardından belgelere erişiyorlar fakat avukatların gördüğü bilgi, belgeyle hâkimin dosyayı görmesi aynı. Bütün bilgi, belgelere erişebiliyorlar. Vekâletnamesi bulunan dosyalar.

HAYDAR AKAR (Kocaeli) – Kendilerine tanınan yetkiler çerçevesinde dosyalara erişebiliyor.

BAŞKAN – Bu arkadaşımız hatırlattı bir konuyu, teşekkür ederiz.

Var mı, devam edecek miyiz?

HAYDAR AKAR (Kocaeli) – Tamam şimdilik.

BAŞKAN – Bu, hani diğer ülkelerde 7/24 sistemi konusu vardı. Biliyorsunuz herhâlde bu konuyu, arkadaşımız hatırlatınca şimdi, o benim de aklıma geldi.

Siz başka ülkelerde bu sistemleri hiç incelediniz mi -Avrupa da olabilir, gelişmiş ülkelerde olabilir, Amerika'da olabilir- hangi birim altında toplamışlar diye o 7/24'ü? Bu sistemin Adalet Bakanlığı içerisinde olması sakınca yaratır mı? Bir onunla ilgili de görüş belirtirseniz seviniriz.

ADALET BAKANLIĞI TETKİK HÂKİMİ MUSTAFA SABİT – 7/24 konusuna ben değinmiştim. 7/24 konusunda biz Hollanda'ya bir çalışma ziyareti gerçekleştirdik. Zira, bu 7/24 Hollanda'da Adalet Bakanlığı bünyesinde, bir de Anglosakson ülkelerde, özellikle Amerika'da Adalet Bakanlığında. Adalet Bakanım henüz bir çalışma ziyareti yapma fırsatımız olmadı ancak Amerika bu açıdan en önemli ülke çünkü -ben kendi istatistiğimizden bahsettim- taleplerimizin yüzde 80'i Amerika'ya gidiyor. Bu bütün ülkeler için aynı. Neticede bütün server'ler orada olduğu için, hemen hemen her ülkenin muhatabı Amerika ve Amerika bu merkezi Adalet Bakanlığı bünyesinde bulunduruyor.

Hollanda'da gördüğümüz husus şuydu: Bu hususta polisle iş birliği kapsamında da talepler geliyor. Bu polisle iş birliği kapsamında gelen taleplerin ve adli iş birliği kapsamında gelen taleplerin ayrımını yapabilecek bir hukuki yardımın mutlaka verilmesi gerekiyor, bu Hollanda'da veriliyor, orada bir savcı gözetiminde yapılıyor bu işler. Bizim Hollanda'da gördüğümüz husus buydu. Yani oradaki gelen olayların hukuki nitelendirmelerinin yapılabilmesi lazım.

Diğer ülkelerde de özellikle Avrupa'da savcılık ve polis iç içe geçtiği için polis kapsamında gözüktüyor bir kısım ülkelerde yani Avrupa'nın çoğu ülkesinde polis veya İçişleri Bakanlığı bünyesinde gözüktüyor ama bunlar aynı zamanda savcılık. Dolayısıyla, aslında bir adli mekanizma kontrolü altında bu 7/24 hizmetleri görülüyor ve nitekim de 7/24 içerisine gelecek taleplere baktığımız zaman, bunun sadece polis kapsamında yürütülmesinin çok riskli olacağını ben söyleyebilirim çünkü bu talepleri -mesela Hollanda için de o şeyi gözlemledim- gönderirken talebi gönderen merkez, özellikle talep alırken pek çok yerden talep alıyorlar, başka bir ülkenin bütün adli makamlarından talep gelebiliyor. Gelen bu taleplerin, mesela Kişisel Veriler Kanunu kapsamında da "Hakikaten karşı tarafın talebi karşılanabilir bir talep midir, her ne kadar siber suç burada hızlı bir irtibat ağı öngörse de gerçekten bu veriler, bir aciliyet gerektiren bir durum var mıdır ve bu

talep sözleşmeye uygun mudur?” Çünkü bunların sonuçları da ağır sonuçlar doğurabilecektir, dolayısıyla bunların mutlaka bir hukuki denetime tabi olması gerektiğini düşünüyoruz.

BAŞKAN – Yani aslında son bölüme katıldığım için -ben de Erdal Aksünger, İzmir Milletvekiliyim Cumhuriyet Halk Partisinden- Haydar Bey’le birlikte daha önce çok konuştuğumuz bir konuydu bu. Biz ilk günden beri bir bilişim bakanlığı kurulması noktasında çaba gösteriyoruz gerçekten de, önerimiz de var. Biz de bilişimciyiz, ikimiz de yani bu sektörün hafızasını bilen adamlardanız.

Özellikle şöyle düşünüyorum: Neden o “Microsoft konusu” dedim? Çünkü zaten dünyanın herhangi bir yerindeki, herhangi bir uluslararası bir şirkete bir ülkenin bütün yazılımını teslim etmek kadar bence ucuz bir hikâye olamaz. Yani o yüzden biz kendi yazılım, database’lerimizi geliştirmemiz lazım, orada da bir bilişim bakanlığı, ülkeyi gerçekten ulusal olarak kabul edebilecek yani bütün data’nın her tarafta yönlendirmesi... Bugün sizde mesela Bulut Bilişim konusu var şu anda. Bence bu da sanal tartışmadır. Neden? Gelecekte işte uydulardan yönetilecek gibi bir durum var zaten içeride ama biz buraya giderken birilerinin yönlendirmesinden, dışarıdan değil, kendi içimizde vereceğimiz stratejilerle bu güvenlikleri sağlamamız lazım. Yani her kurumun böyle dertleri var, biliyoruz; işte sizin de bahsettiğiniz, işte birileri gelecek, burada bir bilişim altyapısıyla ilgili sizlere destek verecek çünkü sizin asli işinizin normalde bu olmaması gerekiyor çünkü oradaki projeyi yürüten kurumlar olması lazım yani bu tarafı yönlendiren değil. Bizim de bu konudaki asıl önerimiz, mevcudiyette Medis de, bir bakanlık altında kurulması gerekli. Ben bunun kaçınılmaz olduğunu düşünen de bir insanım zaten. Araştırmaları da arkadaşlarımız yaptı, 42 ülkedeydi galiba, 42 ülkede zaten böyle bir yapılanma süreçleri yaşanmış. Bu şunu getirecektir bir tarafından: Güvenliği tabii bir yerde toplamak çok önemli de, önümüzdeki on yıllık plan içerisinde ulusal bir yazım, database’yle, bunun, güvenliklerimiz de kendi yazılımlarımız da dâhil olmak üzere bir elden yönlendirilip yönetilmesi.

Şimdi elektronik imzaya geçeceksiniz, size bu elektronik imza altyapısını yazan yine bir uluslararası bir şirket. Onun tersini yapabilecek de o zaten normalde bakarsanız. Yani böyle bir tehditle zaten dünya karşı karşıya. Bunu hep kitlemeye çalışıyoruz şu anda. Ne oluyor? Siber saldırılar olduğunda -beraber tartıştığımız bir konuydu- hacker’ları adam görüyor, bu hacker’ı kendi bünyesine alarak bu işi çözüyor. Normalde iş böyle yürüyor. O yüzden hani, yaptığınız öneri, özellikle en sonunda değindiğiniz öneri, bizim iddia ettiğimiz bir öneridir zaten bir...

HAYDAR AKAR (Kocaeli) – Öneriler doğrumu?

BAŞKAN – Doğru, yani ama temeli bir toplanmadır, kendimizin, hani bütün ulusal olarak bunu kabul edecek bir bilişim bakanlığının kurulması, bu işinin, gücünün her tarafta bir vesileyle bunları yönetecek ve yönlendirecek iç piyasayı da buna adapte ettirecek bir sistematığın ve bir projenin hazırlanması olarak görüyoruz.

Başka soru varsa alalım.

Haydar Bey, bir şey söyleyecektiniz.

HAYDAR AKAR (Kocaeli) – Yok, seni tamamlamak için söyleyecektim.

BAŞKAN – Yani, biz aynı fikirde olduğumuz için yani bununla ilgili oturup çok konuşuyoruz, katkı koymak açısından söyledim bunların hepsini. Önerilerinizi ben de doğru buluyorum kendi açınızdan baktığınızda, farklı öneriler.

Buyurun.

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Teşekkür ederim Sayın Başkan.

Arkadaşıma, meslektaşına destek anlamında ve buna ilave bir kısım teklifler, belki öneriler ifade etme adına şunu belirtmek isterim. Belki de daha evvelden dinlemiş olduğunuz uzmanların da belki bu yönde, paralel teklifleri de olmuş olabilir.

Siber Suçlar Sözleşmesi'nin 9'uncu maddesi pornografiyi düzenliyor. Bizim de buna mukabil gelen Türk Ceza Kanunu'muzda müstehcenlik maddesi var 226'ncı madde ancak biz bunu incelediğimizde, her ne kadar şu anda Siber Suçlar Sözleşmesi imzalanmış ancak onaylanmamış olsa bile, çok kısa zamanda onaylama safhasından sonra tabii iç mevzuatımızda bir uyumluluk çalışmasını gerektirecek fakat şu aşamada bile bir kısım faaliyetler -ki hassas faaliyetler bunlar- toplumun vicdanını yaralayabilecek faaliyetler, şu anda bizim iç mevzuatımızda karşılanmadığını görüyoruz. Mesela pornografik faaliyetlerin Siber Suçlar Sözleşmesi'nde her türlü tanımlanmış iken maalesef sadece Türk Ceza Kanunu'nun 226'ncı maddesinde "müstehcenlik" başlığında tanımlandığından bir kısım faaliyetler cezalandırılmıyor. Mesela ne gibi? Bir çocuk sesinin pornografik bir eyleme dâhil edilmesi gibi, mesela bir çocukla bir hayvan ilişkisinin tasvir edilmesi gibi, mesela bir çizgi film veyahut da animasyonda gene aynı şekilde, bir pornografik faaliyet içerisinde bir çocuğun gösterilmesi gibi eylemler şu anda Türk Ceza Kanunu'nda suç olarak tanımlanmamış. Bir bu problemimiz var.

BAŞKAN – Onları bize aslında öneri olarak getirirseniz, çok iyi olur. Bunu yazılı bir öneriye döndürün, arkadaşlarımız bunu alsınlar, önemli bunlar bence de.

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Sayın Başkanım, burada bir de gerçekten çok önemli başka bir husus daha var. Ki gerçekten bu belki de birincisinden çok daha temel bir mevzu. Maalesef Siber Suçlar Sözleşmesi bizim iç hukukumuzda - her ne kadar arkadaşımız söyledi- belki yüzde 80 itibarıyla dâhil edilmiş, hâlihazırda olsa bile, bu temel, Türk Ceza Kanunu'nun mantalitesi içerisinde aktarıldığı için siber âlemin bir kısım kendine has özellikleri de, genel suçlara ilişkin bir kısım özelliklere de uymadığından ötürü genel ceza maddeleriyle bunları düzenlemek mümkün değil. Mesela ne gibi? Mesela, verinin eşya olup olmadığı hususu tartışılıyor şu anda akademik çevrelerde ve bu konuda da zaten bir ittifak var, bunun eşya olmadığı yönünde. Dolayısıyla, bu eşya olmadığı takdirde, Türk Ceza Kanunu 54'üncü maddesi uyarınca pornografik bir materyalin, suçtan elde edilmiş olan bir madde ve eşya veya suçta kullanılan bir madde ve eşya olarak tanımlanıp müsaderesinde sıkıntı var çünkü TCK 54'üncü maddesinde açık olarak "eşya" diyor fakat sizin o "pornografik materyal" diyebileceğiniz şey bir maddi cismi olan bir şey değil, orada verilerden bahsediyoruz. Dolayısıyla, bu verinin, esasen hukuken el konulması ve her türlü siber suçun işlenmesinde kullanılan verilerin el konulması zapt edilmesi hususunda veri, maalesef TCK'da "eşya" olarak tanımlanmadığı için bir sıkıntı var.

BAŞKAN – Eşya olarak tanımlanmaya mı ihtiyaç var?

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Evet.

BAŞKAN – Bence onu not alalım o zaman. Yani bence de doğru onun “eşya” olarak tanımlanmasıysa. Çünkü niye? Onu çıktı alırsanız eşyaya dönmüş oluyor, değil mi yani öyle bir durum var.

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Evet.

BAŞKAN – Orada durduğu zaman eşya olarak tanımlanmıyorsa onu çıktı olarak aldığınızda eşyaya dönüyor. O zaman bence onu da biz not alalım arkadaşlar.

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT – Teşekkür ederim.

BAŞKAN - Evet, bu önerilerin devamında olanları da alırsak arkadaşlarımız burada değerlendirir.

Başka var mı? Arkadaşlar, var mı?

Sayın Başkan, var mı bir şey?

(Oturum Başkanlığına Komisyon Başkanı Adana Milletvekili Necdet Ünüvar geçti)

BAŞKAN – Bu şey soruldu mu acaba, bilişim, ihtisas mahkemeleri.

Kusura bakmayın, bir yoklama için gitmem gerekti.

Bu hep bilişim ihtisas mahkemeleri, Değerli Genel Müdürüm, hep konuşuluyor yani “Böyle bir ihtisas mahkemesi kurulsun.” diye. Sizin gündeminizde böyle bir şey var mı?

Bir de şöyle enteresan bir husus oldu bu hafta pazartesi günü. Bir grup İnternet içerik sağlayıcısıyla toplantı yaptık ve çok enteresan bir şeyden bahsetti. Bir ilde bir siteyle ilgili, bu maç sonuçlarını veren bir siteyle ilgili bir konu gündeme geliyor ve 2 defa aynı bilişim polisinin bilirkişilik yaptığı bir ortamda şey oluyor, “Ya, bunlar illegal bahis oynatan site.” filan deniliyor. Daha sonra, işte yargı kararıyla kapanıyor, hatta kendisine de bildirimde bulunuluyor o siteyi takip edenler üzerinden haber oluyor.

Burada şöyle bir şey çıkıyor enteresan -tabii bu örnekler çok fazla veriliyor-: Bizim mutlaka hâkim ve savcılarımıza bu bilişim okuryazarlığı anlamında ciddi bir çalışma yapmamız gerekiyor. Bir bunu yapmak lazım, bir de bilişim suçlarıyla ilgili çalışan ihtisas mahkemelerinin kurulması gerektiği hep gündeme geliyor. Bu konuda kanaatlerinizi almak isterim açıkçası.

ADALET BAKANLIĞI ULUSLARARASI HUKUK VE DIŞ İLİŞKİLER GENEL MÜDÜRÜ DR.
NURDAN OKUR – Sayın Başkanım, bilişim ihtisas mahkemelerinin kurulması gerektiği yönünde ben kişisel olarak size katılıyorum ve tartışmalar da var ancak Adalet Bakanlığının gündeminde şu anda öyle bir şey yok. Biliyorsunuz, mahkemelerin kurulması Adalet Bakanlığının teklifi üzerine HSYK tarafından yapılıyor. Şu an öncelikli olarak hem HSYK’nın hem Adalet Bakanlığının, gerek eğitim faaliyetleri gerekse iş yükünün azaltılması konusunda çalışmaları öncelikli olduğu için bu konuda bir çalışma olduğunu bilmiyorum.

BAŞKAN – Biz bunu Komisyon raporumuza koyacağız yani haberiniz olsun, bunu koyacağız.

ADALET BAKANLIĞI ULUSLARARASI HUKUK VE DIŞ İLİŞKİLER GENEL MÜDÜRÜ DR.
NURDAN OKUR – Tabii, tabii...

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Sayın Başkanım, teşekkür ederim.

Sayın Başkanım, bu konuda tartışmalar uzun süredir devam ediyor ancak yani mahkeme, özel ihtisas mahkemesi kurulması aşamasına gelmiş olmasa bile şu anda Ankara'da 6 cumhuriyet savcısı bilişim savcısı olarak özel olarak yetkilendirilmiş durumda. Gene İzmir'de ve İstanbul'da da belli bir sayıda savcılarımız özel olarak Siber Suçlar Sözleşmesi'nin soruşturulmasından görevli vaziyette.

Tabii ihtisas mahkemelerinin kurulmasının önünde pratik bir kısım ön yargılar var, şöyle ki: "Tabii, birçok yerde siber suç yani siber suçun işlenmesi söz konusu fakat bunların belli yerlerde kurulması hâlinde delillerin o mahkemelere sadece getirilebilmesi bir zorluk arz edecek." gibi bir kısım da görüşler var ancak tabii soruşturma aşamasında...

BAŞKAN – Bölge ihtisas mahkemesi kurulsa olmaz mı? Mesela yani Türkiye'nin üç bölgesinde kurarsınız, yani hiç olmazsa bir başlangıç olur. Böyle bir şey olmaz mı?

ULUSLARARASI HUKUK VE DIŞİLİŞKİLER GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI
LEVENT KURT - Böyle bir şey olabilir. Zaten soruşturma aşamasında en önemli olan husus, malumunuz, delillerin elde edilmesi hâlinde siber suçun cezalandırılması mümkün hâle gelebilecek. Bu safhada alınan bir tedbir yani bir savcının veyahut da işte polis memurlarının veyahut da diğer emniyet güçlerinin o konuda gerekli eğitimi almış olmaları ve eğitilmeleri, delilleri güzel toplamaları demek, zaten dosyanın mahkemenin önüne getirilebilmesi anlamına gelecek. Belki hani, özel ihtisas mahkemelerinin kurulmasından daha da öncelikli bir husus. İşte, az önce de söylediğim gibi, savcılık anlamında bu şekilde bir ihtisaslaşmaya gidilmiş durumda. Polis hususunda da zaten malumunuz, özel birimler var siber suçların soruşturulmasından görevli.

Bir de bu konuda bizim yaptığımız bir kısım çalışmalar var, eğitim çalışmaları, özellikle savcı ve hâkimlerimize yönelik. Daha çok yeni 25 kadar savcımızı, Avrupa Konseyi ve Avrupa Birliği, Adalet Bakanlığıyla birlikte yaptığımız bir projede kendilerini davet ettik ve onlara siber suçlar konusunda bir eğitim vermiş bulunmaktayız ve ayrıca Adalet Akademisinde de aynı şekilde düzenli olarak eğitimler kendilerine verilmektedir.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Bir şey ilave edebilir miyim.

BAŞKAN – Buyurun.

ADALET BAKANLIĞI BİLGİ İŞLEM DAİRESİ BAŞKANI MESUT ORTA – Tabii ki mahkemeler çok önemli ancak mahkemeye getirilen deliller, CMK 134 kapsamında hem arama izni verilirken de şu anda özel nitelikte kabul edildiği için, mahkeme tarafından verilen arama kararlarının içerisinde bilgisayarlarda arama ayrı bir usule tabi. Hâkimin ayrıca onu belirtmesi gerekiyor. Belki günümüzde her arama yapılan evde mutlaka bir bilgisayar ya da bilişim cihazı var. Belki buradaki usullerle, kolluk bu konuda daha fazla eğitim almalı diye düşünüyorum çünkü mahkemeye gelen bilişim delillerinin incelenmesi ve bunların düzgün şekilde mahkemelere intikal etmesi, mahkemenin vereceği kararı çok büyük oranda etkilemektedir. Bu konuda büyük eksiklik olduğunu düşünüyorum şahsen.

Teşekkür ederim.

BAŞKAN – Teşekkürler.

ADALET BAKANLIĞI ULUSLARARASI HUKUK VE DIŞ İLİŞKİLER GENEL MÜDÜRÜ DR. NURDAN OKUR – Sayın Başkanım, bir şey ilave edebilir miyim.

BAŞKAN – Buyurun Sayın Genel Müdürüm.

ADALET BAKANLIĞI ULUSLARARASI HUKUK VE DIŞ İLİŞKİLER GENEL MÜDÜRÜ DR. NURDAN OKUR – Şimdi burada tartışılan konulara bakılınca, siber suçların özellikle hukuki niteliğine baktığımızda gerçekten mahkemelere intikal edecek delillerin çok önem arz ettiği ortaya çıkıyor. Bu anlamda ben tekrar vurgu yapmak istiyorum, 35’inci madde anlamında, merkezî makamın, mutlaka hukukçu gözetiminde yapılması gerekiyor ve uluslararası adli yardımlaşmada Adalet Bakanlığı yetkili. Şayet ikinci olarak yani İçişleri Bakanlığında kalacaksa mutlaka yine irtibatlı olarak hukuki açıdan gözden geçirilmesi gerektiğini düşünüyorum.

Teşekkür ederim.

BAŞKAN – Teşekkürler, sağ olun.

Erol Bey, bir şey söylüyor musunuz?

EROL DORA (Mardin) – Yok.

BAŞKAN – Erdal Bey?

ERDAL AKSÜNGER (İzmir) – Yok.

BAŞKAN – Herhâlde bu kişisel verileri falan konuştunuz?

ERDAL AKSÜNGER (İzmir) – Konuştuk, genelde mantık olarak aynı.

BAŞKAN – Buna herkesin inandığı, kabul ettiği ve olması gerektiği hâlde bu niçin çıkmıyor, ben bir türlü anlamış değilim yani.

ADALET BAKANLIĞI KANUNLAR GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI DR. MUSTAFA TAŞKIN – Sayın Başkanım, çok haklısınız, biz de aynı şeyi düşünüyoruz. Neredeyse yirmi yıllık bir geçmiş var ancak bir türlü yasalaştıramadık. Aslında bu kanun, fişlemeleri –kabaca tabiriyle- önlemek için gelen bir kanun. Şu an için bu alanı düzenleyen doğru dürüst mevzuatımız yok, bu alanı kontrol eden bir otoritemiz yok; bütün piyasasını düzenleyen kurumlarımız var, alkol piyasasını düzenleyen kurumlarımız var, veri alanını düzenleyen kurumumuz yok. Bundan dolayı biz Avrupa ülkeleri nezdinde “güvenilmez ülke” olarak nitelendiriliyoruz ve biz onlara şu an, veri paylaşımı gündeme geldiğinde vermek durumundayız ancak onlar bize vermiyorlar. “Siz bu alanda yeterli koruma mekanizması kurmamışsınız, ülke olarak güvenilmez ülkesiniz.” diyorlar, vermiyorlar. Yani bu sıkıntıdan bir an önce kurtulmamız gerekiyor. Kanunun kendisi, fişlemeleri, yasa dışı kayıtları, istismarı önlemek için getirilmiş olmasına rağmen maalesef kamuoyunda sanki devletin veya kamu kurumlarının bu kanunla birtakım fişlemeler, yanlış istismarlar yapacağı gibi bir algı oluştu, olumsuz bir algı oluştu.

Burada şu sorun biraz belki buna kaynak teşkil etti: Tercüme ağırlıklı bir kanundu önceki kanunumuz. Şu an tamamen onu gidermeye yönelik biz bir çalışma yaptık. Umuyoruz, yeni göndereceğimiz...

BAŞKAN – Siz bitirdiniz, Başbakanlığa gönderdiniz, değil mi?

ADALET BAKANLIĞI KANUNLAR GENEL MÜDÜRLÜĞÜ DAİRE BAŞKANI DR. MUSTAFA TAŞKIN - Şu an resmî metin, Başbakanlıktaki resmî metin daha önce Meclisimize de gelmiş olan metin ancak biz ayrı bir çalışma daha yaptık şu an, tamamen hem Avrupa Birliği mevzuatını, müktesebatını karşılayacak hem iç hukukumuzdaki terminoloji anlamında, müesseseler anlamında daha iyi oturan bir metin hazırladık. İlgili uzmanlarıyla paylaştık, hocalarımızla görüştük. Yakın bir zamanda Başbakanlıktaki metinle bu metni mezc ederek Meclise göndereceğiz.

BAŞKAN – Tamam, inşallah, bekliyoruz.

Çok teşekkür ediyorum, çok güzel, verimli...

ERDAL AKSÜNGER (İzmir) – Ben de “Bu metni hazırladınız mı?” diye soracaktım, cevabını verdi.

BAŞKAN – Teşekkür ediyorum.

Kapanma Saati: 16.32