



# USULİ GÜVENCELER SAĞLANIRKEN SİBER SUÇLARLA ETKİLİ MÜCADELEDE KARŞILAŞILAN ZORLUKLARA İLİŞKİN YAPILAN YUVARLAK MASA TOPLANTISI RAPORU

## Danışmanlar

Esther George  
Hasan Sınar  
Maria Andriani Kostopoulou  
Murat Volkan Dülger  
Veli Özer Özbek

*Bu raporda dile getirilen görüş ve düşünceler yazarların kişisel görüşleri olup Avrupa Birliği, Avrupa Konseyi, Adalet Bakanlığı veya projenin diğer paydaş kurumlarının resmi görüşü olarak algılanmamalıdır.*

Bu rapor Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilen ve Avrupa Konseyi tarafından yürütülen **Türkiye’de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması** Avrupa Birliği - Avrupa Konseyi Ortak Projesi kapsamında hazırlanmıştır.

Projenin Sözleşme Makamı Merkezi Finans ve İhale Birimidir.



## İçindekiler

A. Arka plan .....	3
B. Giriş .....	3
C. Toplantı Hakkında Genel Değerlendirmeler .....	3
1. Bilişim Suçlarının Soruşturulması ve Dijital Delillerin Elde Edilmesi ve Kullanılması.....	3
2. Bilişim Suçlarının Nitelendirilmesi .....	4
3. Kişisel Verilerin Korunmasının Bilişim Suçlarıyla Mücadelede Etkisi .....	5
4. İnternet Aracılığıyla İşlenen Cinsel İstismar Suçları .....	5
D. ÖNERİLER .....	5
1. Bilişim Suçlarının Soruşturulması ve Dijital Delillerin Elde Edilmesi ve Kullanılması.....	5
2. Bilişim Suçlarının Nitelendirilmesi .....	7
3. Kişisel Verilerin Korunmasının Bilişim Suçlarıyla Mücadelede Etkisi .....	7
4. İnternet Aracılığıyla İşlenen Cinsel İstismar Suçları .....	7
5. Somut Tavsiyeler .....	8
EK: Toplantı Programı .....	10

### Kısaltmalar:

AİHM	Avrupa İnsan Hakları Mahkemesi
BAM	Bölge Adliye Mahkemeleri
BDDK	Bankacılık Düzenleme ve Denetleme Kurulu
CMK	Ceza Muhakemesi Kanunu
INTERPOL	Uluslararası Kriminal Polis Teşkilatı
KVKK	Kişisel Verilerin Korunması Kanunu
TCK	Türk Ceza Kanunu
UYAP	Ulusal Yargı Ağı Bilişim Sistemi

## A. ARKA PLAN

Bu rapor, Türkiye’de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi ihlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması Ortak Projesi kapsamında gerçekleştirilen Usuli Güvenceler Sağlanırken Siber Suçlarla Etkili Mücadelede Karşılaşılan Zorluklara ilişkin 26-27 Şubat 2020 tarihlerinde İzmir’de gerçekleşen Yuvarlak Masa Toplantısı’na ilişkindir.

Projenin ana faaliyet alanları aşağıda belirtilmektedir:

- Ceza adaleti alanında ihtiyaç analizi,
- İnsan hakları alanında ceza adaleti kapasitesinin geliştirilmesi,
- İnsan hakları alanında çeşitli farkındalık artırıcı etkinliklerin düzenlenmesi.

## B. GİRİŞ

Bu rapor, ceza adalet sisteminin güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi ihlallerinin önlenmesi için yargı mensuplarının kapasitesinin artırılması bağlamında siber suçların soruşturulması ve kovuşturulması ile dijital delillerin elde edilmesi özelinde, uygulamada hem soruşturma, hem de karar verme sürecinde ortaya çıkan sorunların, ihtiyaçların ve çözüm önerilerinin analiz edilmesi amacıyla kaleme alınmıştır.

Bu rapor, Esther George, Hasan Sınar, Maria Andriani Kostopoulou, Murat Volkan Dülger ve Veli Özer Özbek tarafından yukarıda bahsi geçen yuvarlak masa toplantısı süresince tutulan notlara dayanmaktadır. Bu notlar, Murat Volkan Dülger tarafından bir araya getirilip, bu ortak raporu meydana getirmiştir. Bu nedenle, raporda sunulan bulgular da ekte sunulan toplantı programında dile getirilen konular ve katılımcılardan edinilen bilgiler ile sınırlıdır.

Toplantı, Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü, Türkiye’nin çeşitli illerinde görev yapan bilişim suçları konusunda çalışan Cumhuriyet savcıları, bölge adliye mahkemesi hakimleri, Yargıtay savcı ve hakimleri, emniyet ve jandarma mensupları, Türkiye Bankalar Birliği, Bilişim Teknolojileri ve İletişim Kurumu ile diğer paydaş kurum çalışanları ve Avrupa Konseyi uzmanlarından oluşan elli bir kişinin katılımı ile gerçekleştirilmiştir.

## C. TOPLANTI HAKKINDA GENEL DEĞERLENDİRMELER

Ulaşılan bulguları 4 ana başlık altında toplamak mümkündür:

### 1. Bilişim Suçlarının Soruşturulması ve Dijital Delillerin Elde Edilmesi ve Kullanılması

- Tüm savcılar, polisler ve Avrupa Konseyi danışmanları CMK m. 134’ün (*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*) yetersiz olduğu konusunda hem fikirdir.

- Polisin topladığı kanıtlar kolaylıkla hukuka aykırı hale gelebilmektedir. Uyulması gereken usullere uygulamada dikkat edilmemektedir.
- Soruşturma aşamasında iş yükü fazlalığı (dosya sayılarında son yıllarda meydana gelen büyük artışlar) doğru ve eksiksiz soruşturma yapılmasını engellemektedir.
- İlk ifadeyi müracaat savcısının alması, polisin yetenek ve imkânlarının geri plana atılmasına yol açıyor. Bu ise mağdura doğru soruların sorulmasını, doğru bilgilerin elde edilmesini ve hızlı hareket edilmesini engellemektedir. Dolayısıyla özellikle bilişim suçlarında ilk ifade ve temas polis tarafından yapılmalıdır.
- Soruşturma aşamasında bilgi toplanacak kurumların iletişim ve iş birliğinin kolaylaştırılması gerekiyor. Örneğin bankalardan yazışma yapılmak suretiyle işlem yapılması işleri çok uzatıyor. Bankacılık sisteminin UYAP'a açılması ise Bankacılık Kanunu gereğince yasak. Bunun için Adalet Bakanlığı ile BDDK arasında bir protokol yapılabilir.
- Bankalardan çekim yapan failler için yüz tanıma sistemlerinin getirilip getirilemeyeceği üzerine düşünceler olsa da şimdilik bu tarz sistemlerin çok pahalı olduğu ve yalnızca polis tarafından kullanıldığı dile getirilmiştir. Ayrıca kişisel verilerin korunması hukuku açısından da sorunlu bir alan oluşturabileceği düşünülmektedir.
- Soruşturma aşamasında henüz inceleme aşamasına gelmediği dile getirilen bilişim suçu dosyaları için savcılık tarafından resmi bilirkişi bulunamamakta ya da polis iş yükünün fazla olduğu gerekçesiyle işlemleri çok geç yapmaktadır. Bu nedenle savcılık tarafından ücreti karşılığında bilirkişiye başvurulduğunda, bu bilirkişilerin de siber suçlarda görevli olan polis memurları olduğu görülmektedir. Dolayısıyla polisin görevi gereği yapması gereken işlemleri bilerek geciktirmek suretiyle dosyaların bilirkişilere gönderilmesini sağladıkları tespit edilmektedir. Bunun bir kazanç kapısı haline geldiği ve hukuk düzeni içerisinde doğru olmadığı görülmektedir.
- Vergi suçlarındaki inceleme şartının (veri suçu raporu) bilişim suçlarında da dava açılması için bir ön şart olarak getirilmesi uygun olabilir; bu rapor olmadan dava açılmaması sağlanabilir.

## 2. Bilişim Suçlarının Nitelendirilmesi

- Yargıtay'ın kararlarında istikrar olmaması, içtihat birliğine varılmamış olması en çok eleştirilen konulardan birisini oluşturuyor.
- Özellikle ilk derece mahkemelerinde uzmanlaşma olmaması eleştiriliyor. Çünkü bilhassa TCK 245/2. ve 3. fıkraları, 245/A, 136 ve 158. maddelerinde suçun nitelendirilmesi farklı sonuçların doğmasına sebep oluyor.
- Son üç yıldır büyük artış gösteren suçlardan birini yasa dışı bahis oluşturmakta ve polis bu suçun örgütlü olarak işlendiği konusunda emin. Dolayısıyla düzenleme ve önlemlerin buna uygun hazırlanması gerekiyor.
- Bazı suçlar için temel cezadaki makas aralığının değişmesi gerekiyor. Haksızlık içeriğine bakılmadan yapılan düzenlemeler eleştiri konusu yapılmakta.

- Özel hayatın gizliliğinin ihlali suçunun kapsamına giren konuların çeşitliliği ve göreceliliği nedeniyle hukuki güvenliğin ve uygulamadaki birliğin sağlanmasında sorunlar yaşanmaktadır.

### 3. Kişisel Verilerin Korunmasının Bilişim Suçlarıyla Mücadelede Etkisi

- İnternet dolandırıcılığı suçunun işlenme sayısı, yayınlanan Interpol istatistiklerine göre her geçen gün artmaktadır.
- Bulut bilişim araçlarının ve hizmetlerinin yaygınlaşması kişisel verilerin ele geçirilmesi ve yayılması konusunda büyük problemleri beraberinde getirmiştir.
- Mağdurların kişisel verilerinin önemi ve bunların korunması gerektiğine ilişkin farkındalıklarının olmaması suç sayısının artmasına yol açmaktadır.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ile TCK birbirine uyumlu değildir.

### 4. İnternet Aracılığıyla İşlenen Cinsel İstismar Suçları

- Çocuk pornografisinde özellikle Whatsapp üzerinden çocukların paylaşımında bulunduğu görülmektedir.
- Polis Deepweb konusunda birçok ülkenin polis teşkilatından daha iyi durumda olduğunu ifade etmektedir.
- TCK m. 226/3 müstehcenlik suçu ile m. 103 cinsel istismar suçu arasında bir ilişki kurulmasının zorunlu olduğunu düşünülmektedir. Direkt olarak çocuk pornografisine dair düzenleme olmaması bir eksikliklerdir.
- Çevrimiçi cinsel istismar ve sömürü suçlarının tanımlarının, iç hukukta, bu konudaki Avrupa Konseyi standartlarını tam olarak yansıtmadığı görülmektedir.
- Emniyet Genel Müdürlüğü nezdinde Avrupa Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi) kapsamında çalışan 7/24 iletişim noktasının varlığı, görevleri ve soruşturmalarda nasıl yardımcı olabileceği konusunda uygulamacılarda büyük bir bilgi eksikliğinin bulunduğu gözlemlenmektedir.

## D. ÖNERİLER

Önerileri de tıpkı yukarıda kategorilere ayrılan bulgular gibi aynı başlıklar altında toplamak mümkündür:

### 1. Bilişim Suçlarının Soruşturulması ve Dijital Delillerin Elde Edilmesi ve Kullanılması

- 1.1. Polisin elinde bilişim suçuyla karşılaştıklarında kullanabilecekleri yapılmaması gerekenlere ilişkin bir "kontrol listesi" olması ve en temel düzeyde yapılması gerekenlerin bu sayede gözden kaçmaması sağlanmalıdır.
- 1.2. Şüphelinin/sanığın ve müdafinin önünde belirli dijital kanıtların ne zaman açılacağı ve bunların toplanma şekli çok önemlidir. Hukuka uygun delil toplama için yol haritası belirlenmeli ve kesin olarak uygulanmalıdır. Elektronik delillerin nasıl ele

alınacağı ve sanık ile avukatına nasıl gösterileceğine dair polisler için bir protokol/kontrol listesinin oluşturulması ele alınabilir.

- 1.3. CMK m. 134 için en kısa sürede katalog suçlar düzenlenmeli ve madde Budapeşte Konvansiyonuna uygun hale getirilmelidir. Her suç için delil toplama farklı özellikler gösterdiğinden, düzenlemede bunun dikkate alınması gerekir.
- 1.4. Ağır iş yükü sorunlarının çözülmesi için hem kolluk hem yargı aşamasında görevli personelin bu konuda eğitilmiş insanlar olmaları ve yargıda kapasitenin arttırılmasına yönelik projelerin yürütülmesi gerekmektedir.
- 1.5. Siber suçlara bakan savcılıkların iş yükünün çok fazla olması nedeniyle, bu makamlarda görev yapan savcı ve diğer personel sayısının artırılması ve yine bu birimlerdeki tüm çalışanlara gerekli teknik bilişim eğitiminin verilmesi gereklidir. Siber suçlara ilişkin savcılık işlemlerinin uzmanlık ve büyük bir deneyim gerektirmesi sebebiyle Hakim ve Savcılar Kurulu tarafından yapılan rotasyonlara bu alanda çalışan savcılarının mümkün olduğunca dahil edilmemesi ve savcılarının bu pozisyonlarda uzun süre görev almasının faydalı olacağı düşünülmektedir. Hâkim ve savcılara yönelik eğitim modülleri hazırlanması gerekir. Bu eğitimlerin kısa, öz ve açıklayıcı olması gerekir (Bilişim savcıları, bilişim ihtisas mahkemesi vs.).
- 1.6. Bu suçlarla mücadelelerde alanında uzmanlaşmış kişilere yer verilmekle beraber devletin bu mesleklere teşvik etmesi de olumlu sonuçlar doğuracaktır.
- 1.7. Emniyet teşkilatında siber suçlara bakan birimlerinin teknik altyapı hizmetleri açısından güçlendirilmesi de öncelikli olarak ele alınmalıdır.
- 1.8. Soruşturma aşamasında bilgi toplanacak kurumların iletişim ve iş birliğinin kolaylaştırılması gerekmektedir. Bu noktada özellikle Türkiye Bankalar Birliği ve Adalet Bakanlığı iş birliğine gitmelidir.
- 1.9. Alanında uzman bankacılar tarafından hâkim ve savcılara yönelik eğitim verilmelidir. Bankacılık ürün ve hizmetlerinin tanıtımı ve bilinen suç tiplerinin tespiti ile ilgili bilgiler paylaşılmalıdır. Adli süreçlerde bankalardan beklenen destek ve bilgilerin de paylaşılması faydalı olacaktır. Bu eğitimler sayesinde ihtiyaç duyulan anlık bilgilere ulaşma konusunda da gelişim sağlanabilir.
- 1.10. Kamu / Özel sektör iş birliğinin özendirilmesi gerekmektedir. Savcılarının bankalardan bilgi almalarını kolaylaştırmak için "Sahteciliği Önleme Çalışma Grubu, Türkiye Bankalar Birliği" ile temas halinde olmaları sağlanabilir.
- 1.11. Emniyet Genel Müdürlüğü nezdinde Avrupa Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi) kapsamında çalışan 7/24 iletişim noktasının varlığı, görevleri ve soruşturmalarda nasıl yardımcı olabileceği konusunda uygulamacılarda büyük bir bilgi eksikliğinin bulunduğu gözlemlenmektedir. Bunun giderilmesi için özellikle savcılara bilgilendirme yapılması gerekir. Ayrıca, siber suçlara bakan savcılıklar ile polis arasında bir işbirliği anlaşması yapılmalıdır.

## 2. Bilişim Suçlarının Nitelendirilmesi

- 2.1. Bilişim suç tiplerinin tespiti ile ilgili bilgiler kurumlar (Türkiye Bankalar Birliği, polis siber suçlar daire başkanlığı, jandarmanın ilgili birimleri ve kovuşturma makamları) arasında detaylı bir şekilde paylaşılmalıdır.
- 2.2. Bulut bilişimde işlenen suçlarda failinin tespiti için, eğer eylem bilişim sistemine yönelik olarak gerçekleştirilmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik gerçekleştirilmişse bu verilerin, hem bilişim sistemine hem de verilere karşı gerçekleştirilmişse her ikisinin ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğu ve zararı kimin meydana getirdiği açıkça ortaya konulmalıdır.
- 2.3. Düzenli aralıklarla hâkim ve savcılar, hatta siber suçları kovuşturan kolluk görevlileri arasında toplantılar yapılarak bilgi paylaşımı sağlanmalıdır.
- 2.4. Suçların temel cezalarında yaptırımların çeşitlendirilmesi gerekmektedir.
- 2.5. Avrupa'daki uygulamalar da örnek alınarak ceza yargılamasındaki dosya yükünü dengelemek ve ciddi meselelere gereken önemi verebilmek için hakaret ve iftira suçlarında cezai takibat yolu yerine hukuki tazminat yoluna gidilmesi, bu eylemlerin suç olmaktan çıkarılması gerekmektedir.
- 2.6. "Bilişim Mahkemeleri" şeklinde siber suçlar ve kişisel veriler alanında ihtisas mahkemelerinin kurulması büyük bir önem arz etmektedir.

## 3. Kişisel Verilerin Korunmasının Bilişim Suçlarıyla Mücadelede Etkisi

- 3.1. Özellikle gençlerin ve ergenlik çağındaki çocukların kendi kişisel verileri hakkında bilgilendirilmesi için okullarda eğitim programları planlanması olumlu sonuçlar doğuracaktır.
- 3.2. Yargı ve kollukta önerilen eğitim modülleri gibi, özel ya da devlet kurum ve kuruluşlarında çalışan tüm personel için de kişisel verilere dair eğitim öngörülmelidir. Bu eğitim ile kişilerin hukuki ve cezai sorumlulukları bildirilmelidir.
- 3.3. Devlet eliyle yürütülen bir soruşturma dahi olsa, kişisel verilerin veri havuzlarından kullanılmasına engel olunmalı, korunması ve kişilerden rıza alınması noktasında kesin uygulama olmalıdır.
- 3.4. Hakim ve savcıların dahi verileri düzgün bir şekilde güvence altına alamamalarının dolayısıyla kendilerini savunmasız duruma getirmelerinin önüne geçilmeli, bu konuda veri korumaya dair eğitim verilmelidir.

## 4. İnternet Aracılığıyla İşlenen Cinsel İstismar Suçları

- 4.1. Bilişim suçlarıyla mücadelede, özellikle çocuklarla ilgili hassas konularda, bu suçların niteliği itibariyle sınırları ve ülkeleri aşan bir yapıda olması nedeniyle uluslararası iş birliği çerçevesinde bu suçların kovuşturulmasında uluslararası yetki sorununun çözülmesi ve iş birliğinin güçlendirilmesi gerekmektedir.
- 4.2. Çocuk pornografisinin ayrı bir suç olarak değerlendirilmesi ve Lanzarote Komisyonunun da görüşüne uygun olarak, istismarın şahsen buluşmanın ötesinde çevrimiçi gerçekleştiği durumları da kapsayacak şekilde düzenleme yapılması gerekmektedir. Haziran 2015 tarihinde Lanzarote Komitesi, bu doğrultuda

ülkelere çocukların cinsel amaçlarla kandırılması (grooming) suçunun kapsamının sadece yüz yüze buluşma sonucu gerçekleşen cinsel istismar durumlarını değil, internet üzerinden işlenen cinsel istismarları da kapsayacak şekilde genişletme çağrısında bulunmuştur.

- 4.3. Daha net ve doğrudan bir müdahale için ayrıca TCK m. 226 ile m. 103 arasında bir ilişki kurulması gerekmektedir.
- 4.4. Çocuklara yönelik bu suçların cezai takibatı boyunca tanık ve mağdurların korunmasına yönelik usul ve esaslar belirlenmeli ve uygulanmalıdır.
- 4.5. Bir başka sorun ise çocuk pornografisi içeren deliller elde edilirken karşılaşılmaktadır. Bu bağlamda, CMK'nın 134. maddesinin icrasına dayalı olarak yaşanan sorunların ortadan kaldırılması gereklidir.
- 4.6. İç hukukun Avrupa Konseyi standartları ışığında yorumlanmasını sağlamak amacıyla, AİHM içtihatlarının da analizleri eklenmek suretiyle, ülkeye özgü materyaller geliştirilebilir ve çevrimiçi çocuk istismarı ile ilgili davalarda bir uygulama rehberine dönüştürülebilir.
- 4.7. Ebeveynler ve bakıcıların da bilişim suçları noktasında genel, çocuklar özelinde de derinlemesine bilgilendirilip eğitilmeleri gerekmektedir.

## 5. Somut Tavsiyeler

Bu bölümde yukarıdaki bulgular ışığında proje kapsamında elde edilebilecek somut çıktılara ilişkin tavsiyelere yer verilmektedir.

- 5.1. Siber suçlar ve elektronik deliller hakkında büyük bir eğitim eksikliğinin olduğu gözlemlenmektedir. Bu sorunun üstesinden gelmek için eğitici eğitimlerinin düzenlenmesi tavsiye edilmektedir. İlerde bu eğitimi alacak kişilere kendi bölgelerinde eğitim verilebilir.
- 5.2. Eğitici eğitimleri ve sıralı eğitimler için ayrı ayrı eğitim modüllerinin hazırlanması faydalı olacaktır.
- 5.3. Proje kapsamında eğitim modülleri ve kılavuzlar hazırlandıktan sonra ülkenin çeşitli bölgelerindeki hâkim ve savcılarının katılımıyla eğitim faaliyetleri yürütülebilir.
- 5.4. Projenin en önemli çıktılarından biri olarak, 2014 yılında tamamlanan "Uygulama Kılavuzu", son gelişmeler ve mevzuat değişiklikleri ışığında güncellenebilir. Bu kılavuzun kendisi ve kılavuza ek olarak sunulan yazışma örnekleri UYAP sistemi vasıtasıyla hakim ve savcılarının erişimine sunulabilir. Bu da projenin en önemli çıktılarından birisi olabilir.
- 5.5. Avrupa Konseyi tarafından hazırlanmış olan e-delil kılavuzunun Türkçe'ye çevrilmesi ve Türkiye bağlamına uyarlanması faydalı olacaktır.
- 5.6. Adli bilişim uzmanlarının desteği ile (özellikle emniyet ve adli tıp görevlilerinin), eğitim modülleri ve uygulama kılavuzunda temel adli bilişim bilgilerine de yer verilebilir.
- 5.7. Proje kapsamında kurulacak bir çalışma grubu vasıtasıyla CMK m. 134 kapsamında yapılacak değişiklik önerileri geliştirilebilir. Bu öneriler, doğrudan Adalet Bakanlığı'na sunulabilir.
- 5.8. Daha önceden bilişim suçları için hazırlanan ve kullanılan kontrol listesi güncellenebilir. Bu kontrol listesi, UYAP üzerinden tüm hâkim ve savcılarının erişimine sunulabilir.



- 5.9. Siber suçlar alanında çalışan ve bu suçlarla ilgilenen savcılar, polisin 7/24 çalışması hakkında bilgilendirilebilir; bu konuda bir broşür hazırlanabilir ve gerekli bilgilere UYAP üzerinden erişim sunulabilir.
- 5.10. Genel Veri Koruma Tüzüğü (GDPR) ve KVKK bağlamında kişisel verilerin korunmasına dair kitapçık hazırlanarak UYAP üzerinde tüm hakim ve savcılarının bu kitapçığa erişmesi sağlanabilir. Ayrıca, eğitim modülleri, bu konu hakkında eğitimi kapsayacak şekilde de düzenlenebilir.
- 5.11. İlgili Yargıtay daireleri ile birlikte bir seminer düzenlenerek, bilişim suçlarına dair içtihadının yeknesaklaştırılması ve içtihat birliğinin sağlanarak uygulanması sağlanabilir. Bunun sonuçları da bir kitapçık haline getirilerek UYAP üzerinden erişim sağlanabilir.
- 5.12. Çocukların cinsel istismarına ilişkin broşürler hazırlanarak Milli Eğitim Bakanlığı işbirliği ile bu broşürlerin okullarda dağıtımı sağlanabilir.
- 5.13. Çocukların çevrimiçi cinsel istismarı ve sömürüsüne ilişkin ulusal mevzuat ve uygulamalarda karşılaşılan eksiklikler ile zorlukların tanımlanması ve bu zorlukların nasıl aşılabileceğinin tanımlanması için (örn. ulusal mevzuatın Avrupa Konseyi standartları ışığında yorumlanması) çalıştaylar düzenlenebilir. Buna ek olarak, Türkiye bağlamında geçerli olan Avrupa Konseyi standartlarına dair ülkeye özgü materyallerin geliştirilmesi de faydalı olacaktır. Çocukların çevrimiçi istismarı davalarına bakan adli makamların somut ve usulü zorunlulukları açısından daha açık bir rehberlik sağlanması için AİHM içtihadının detaylı bir analizi de sağlanabilir. Bunun için, gerekli kılavuz, kontrol listesi veya diğer materyallerin hazırlanması ele alınabilir.
- 5.14. Siber suçların önlenmesi ve siber suçlar hakkında eğitim stratejisinin oluşturulması gereklidir. Bu şekilde siber suçlar bağlamında karşı karşıya kalabilecekleri tehlikeler hakkında toplumun bilinci artırılabilir. Çocuklar ve gençler için siber suçların önlenmesi ve siber güvenlik hususlarında eğitim programlarının düzenlenmesi gereklidir. Türkiye’de zamanla siber suçlar hakkında eğitilmiş bir işgücünün oluşması için üniversitelerde siber suçların önlenmesi ve siber güvenlik hususlarında eğitim verilmesi teşvik edilmelidir.
- 5.15. Hakim ve savcılar tarafından çevrimiçi veri güvenliği derslerinin düzenlenmelidir
- 5.16. Kamu/özel sektör işbirliğinin desteklenmesi. Savcılarının bankalardan bilgi edinme noktasında bazı zorluklar ile karşılaştıkları ifade edilmiştir. “Dolandırıcılığın Önlenmesine Yönelik Çalışma Grubu, Türkiye Bankalar Birliğinin” bankalardan bilgi edinmek isteyen savcılar için irtibat noktası haline getirilmesine yönelik çalışmalar yapılmalıdır. Türkiye Bankalar Birliği, savcılık ve polis arasında bir işbirliği anlaşması yapılabilir.
- 5.17. Siber suçlara bakan savcılık bürolarıyla polis arasında bir işbirliği anlaşması yapılmalıdır. İrtibat noktalarının belirlenmesi için proje kapsamında koordinasyon toplantılarının yapılması faydalı olacaktır.

## EK: TOPLANTI PROGRAMI

26 Şubat 2020

Grand Efes 2

Çarşamba

Salonu

09.00 Kayıt

09.30 **Açış Konuşmaları**

Elena Jovanovska-Brezoska, *Proje Koordinatörü, Avrupa Konseyi, İnsan Hakları Ulusal Uygulamalar Bölümü*

Kamil Erkut Güre, *İzmir Cumhuriyet Başsavcısı*

Şenol Taş, *Ceza İşleri Genel Müdür Yardımcısı, Adalet Bakanlığı*

09.45 **Sunuş Konuşmaları**

**Bilişim Suçları ve İnternet Yoluyla İşlenen Suçlarla Mücadelede Karşılaşılan Temel Zorluklar, Türk Ceza Hukuku Uygulaması ve İyi Uygulama Örnekleri**

Mahmut Kaan Yüksel, *Ankara Cumhuriyet Savcısı*

10.15 *Kahve Arası*

10.30 **Birinci Oturum: Elektronik Delillerin Değerlendirilmesi ve Kabul Edilebilirliği - İyi Uygulama Örnekleri ve Karşılaşılan Zorluklar**

*Oturum Başkanı:* Doç. Dr. Hasan Sınar, *Ulusal Danışman, Avrupa Konseyi*

*Konuşmacılar:*

Esther George, *Uluslararası Danışman, Avrupa Konseyi*

Doç. Dr. Murat Volkan Dülger, *Ulusal Danışman, Avrupa Konseyi*

Furkan Yılmaz, *Başkomiser, Ankara Emniyet Genel Müdürlüğü*

Ahmet Gül, *Yargıtay Cumhuriyet Savcısı*

12.00 Tartışma, Soru–Cevap

12.30 *Öğle Yemeği*

**13.30 İkinci Oturum: İnternet Üzerinden İşlenen Dolandırıcılık Suçları**

*Oturum Başkanı: Doç. Dr. Murat Volkan Dülger, Ulusal Danışman, Avrupa Konseyi*

*Konuşmacılar:*

*Doç. Dr. Hasan Sinar, Ulusal Danışman, Avrupa Konseyi*

*Fatma Aydın Khalil, Dolandırıcılıkların Önlenmesi Çalışma Grubu Başkanı, Türkiye Bankalar Birliği*

*Erden Şahin, Emniyet Amiri, Ankara Emniyet Genel Müdürlüğü, Soruşturma Şube Müdürlüğü*

14.30 Tartışma, Soru–Cevap

15.00 *Kahve Arası*

**15.20 Üçüncü Oturum: İnternet üzerinden çocuk istismarı ve tacizi (Uluslararası standartlar, ulusal uygulamalar, soruşturmada yaşanan zorluklar)**

*Oturum Başkanı: Doç. Dr. Hasan Sinar, Ulusal Danışman, Avrupa Konseyi*

*Konuşmacılar:*

*Dr. Maria Andriani Kostopoulou, Uluslararası Danışman, Avrupa Konseyi*

*Prof. Dr. Veli Özer Özbek, Ulusal Danışman, Avrupa Konseyi*

*Adem Can, Ankara Cumhuriyet Savcısı*

16.20 Tartışma, Soru–Cevap

17:00 **Birinci Gün Sonu**

- 09.30 **Dördüncü Oturum: Siber Suçlarla Mücadelede Kişisel Verilerin Korunması**  
*Oturum Başkanı: Doç. Dr. Murat Volkan Dülger, Ulusal Danışman, Avrupa Konseyi*  
*Konuşmacılar:*  
*Esther George, Uluslararası Danışman, Avrupa Konseyi*  
*Doç. Dr. Hasan Sınar, Ulusal Danışman, Avrupa Konseyi*  
*Mahmut Esat Yıldırım, Siber Güvenlik Uzmanı, Bilgi Teknolojileri ve İletişim Kurumu,*  
*Bilgi Teknolojileri Daire Başkanlığı*
- 10.45 *Kahve Arası*
- 11.00 Tartışma, Soru – Cevap
- 12:00 **Gelişime yönelik tavsiyeler**  
*Doç. Dr. Volkan Dülger, Ulusal Danışman, Avrupa Konseyi*
- 12.45 **Kapanış Konuşmaları**  
*Şenol Taş, Ceza İşleri Genel Müdür Yardımcısı, Adalet Bakanlığı*
- 13.00 *Öğle Yemeği*
- 14.00 **Program sonu**