

**Siber Suçlarla Mücadele Semineri (Abant/Bolu) 23-24 Ekim 2008**

Katılımcılar tarafından, Türk yasal mevzuatının bilişim suçlarına ilişkin hükümleri, bunların Siber Suç Sözleşmesi'ne uyumluluğu ve Sözleşme'ye katılımın muhtemel etkileri konuları üzerinde ayrıntılı sunum ve tartışmalar gerçekleştirilmiştir.

Yapılan sunumlar ve ortaya konan görüşlerin zengin içeriği aşağıdakileri göstermiştir:

- Bu konular, bu alanda geniş bilgi ve deneyime sahip hukukçular ve uzmanlar tarafından derinlemesine değerlendirilmektedir.
- Türkiye'de bilişim suçlarının varlığı ve bu konuya ilişkin mücadelenin topluma önemi konusundaki farkındalıktaki artış dikkat çekicidir. Bu husus, özellikle yargı için geçerlidir.
- Mevcut mevzuat Sözleşme gereklerinin birçoğunu karşılamaktadır. Kaldı ki, olabildiğince az olmak kaydıyla belirli konularda çekince sunma imkanı da gözönünde bulundurulmalıdır.
- Türkiye, ceza kanununda bazı değişiklikleri yapmak suretiyle, Sözleşme'yi onaylayabilir.
- Mevzuatın değişiklik ihtiyacı gösterdiği diğer bazı alanlar da bulunmaktadır (kişisel verilerin korunmasına ilişkin yasanın çıkartılması gibi). Seminer süresince yapılan sunumlar, Devlet ve ilgili resmi mercilere bu alanların belirlenmesi ve mümkün olan hukuki çözümlerin geliştirilmesi konusunda fikir verebilecektir.
- Bilişim suçlarına karşı kamu ve özel sektör arasında işbirliği gösterilmesi elzemdir. Bu husus, özel sektör tarafından bu eğitim seminerine verilen destekle de gösterilmiştir. Seminer'de, Avrupa Konseyi tarafından Nisan 2008'de hazırlanan "Bilişim Suçlarının Soruşturulmasında Soruşturma Mercileri-Servis Sağlayıcılar Arasındaki İşbirliği'ne İlişkin Kılavuz" da dahil olmak üzere iyi uygulamalar konularına değinilmiştir.
- Siber Suç Sözleşmesi'nin onaylanması, Türkiye'nin diğer ülkelerle etkin bir biçimde işbirliği içinde olması için gereklidir.

Sonraki adımlar olarak:

- C. Savcısı ve hakimlere eğitimler düzenlenmeye devam edilmeli ve bilişim suçları eğitim programlarında bir konu başlığı haline getirilmelidir. Yargı, kolluk kuvveti özel sektör arasında multi-disipliner yaklaşım sürdürülmelidir.
- Türkiye, Siber Suç Sözleşmesi'ni mümkün olan en kısa zamanda imzalamalıdır.
- Mevzuattaki eksiklerin giderilmesi, daha etkin yasa hükümlerinin uygulanabilmesi ve Türkiye'nin Sözleşme'ye taraf olmasını kolaylaştıracak çalışmaların hızlandırılması gerekmektedir.
- Acil durumlarda polisin uluslararası düzeyde işbirliği göstermesinin sağlanabilmesi için 24/7 irtibat noktası acilen tesis edilmelidir.
- Kamu ve özel sektör arasındaki işbirliği elde edilebilmesi için Bilişim Suçlarının Soruşturulmasında Soruşturma Mercileri-Servis Sağlayıcılar Arasındaki İşbirliği'ne İlişkin Kılavuz'dan yararlanılabilir.

**Seminar on Cybercrime (Abant/Bolu) 23-24 October 2008**

Participants delivered presentations and discussed in detail the current Turkish legislation related to cybercrime, its compatibility with the Convention on Cybercrime and the implications of this treaty for Turkey.

The quality of the presentations and deliberations clearly showed that:

- These questions have been analysed in depth by legal experts in Turkey, who demonstrated a high level of expertise and knowledge.
- A considerable increase in the awareness of cybercrime and the importance of this issue for Turkish society is noticeable. This is particularly true for the judiciary.
- The current legislation meets most of the requirements of the Convention, at least at a minimum level and if the possibility of reservations that can be made is considered.
- With some amendments to criminal law, Turkey could ratify the Convention.
- There is a range of areas where legislation could be further improved (such as protection of personal data). The presentations made during the Seminar will certainly help the Government and the relevant authorities to identify these areas and possible legal solutions.
- Public-private cooperation against cybercrime is essential. It has been demonstrated by the support provided by industry to this training seminar. Good practices presented during the seminar included the “guidelines for law enforcement – Internet service provider cooperation in the investigation of cybercrime” of the Council of Europe in April 2008.
- Ratification of the Convention on Cybercrime by Turkey is necessary to permit Turkey to cooperate internationally with other countries in an efficient manner.

In terms of the way ahead:

- Further training courses for judges and prosecutors should be organized and consideration should be given to making cybercrime a topic in the training curricula for them. Multi-disciplinary approach with involvement from judges, law enforcement, industry should be maintained.
- Turkey should sign the Convention on Cybercrime as quickly as possible.
- Work on the further improvement of the legislation should be accelerated to close gaps, make the legislation more efficient/effective and allow Turkey to ratify the Convention.
- A 24/7 point of contact should be established as soon as possible to facilitate international police cooperation in urgent cases.
- The guidelines for law enforcement – ISP cooperation could be used to facilitate public-private cooperation in the investigation of cybercrime.