REPORT of ROUNDTABLE MEETING on

CHALLENGES IN FIGHTING CYBERCRIME EFFECTIVELY WHILE ENSURING PROCEDURAL SAFEGUARDS

Consultants:

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

The opinions expressed in this report are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe, European Union, Ministry of Justice or other stakeholders of the project.

This report was prepared under the Joint Project on "Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Turkey," which is co-financed by the European Union and the Council of Europe, and implemented by the Council of Europe.

The Central Finance and Contracts Unit is the Contracting Authority of this Project.

İçindekiler

Abbreviations:

BDDK (BRSA)	Turkish Banking Regulation and Supervision Agency
CPC	Criminal Procedure Code
CoE	Council of Europe
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation
INTERPOL	The International Criminal Police Organisation
IT	Information Technology
ECtHR	European Court of Human Rights
EU	European Union
KVKK	Personal Data Protection Authority
TCC	Turkish Criminal Code
UYAP	National Judiciary Informatics System

A. Background

This report is based on roundtable meeting on Challenges in Fighting Cybercrime Effectively While Ensuring Procedural Safeguards organised between 26 and 27 February 2020 in Izmir relating to the CoE/EU project on "Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Turkey".

The project has identified areas of delivery, which include;

- Needs assessment in the field of criminal justice,
- Capacity building in the field of human rights related to criminal justice,
- Organising awareness raising events in various forms in the field of human rights.

B. Introduction

This report aims to analyse the problems, needs, requirements and solutions that arise in practice, both in the investigation and judgement process, in order to strengthen the justice system and prevent the violations of the ECHR which relate to investigate and judge cybercrime and to obtain digital evidence in practice.

This report is based on consolidation of notes made by Esther George, Hasan Sınar, Maria Andriani Kostopoulou, Murat Volkan Dülger and Veli Özer Özbek in relation to abovementioned roundtable meeting. These notes are incorporated and finalized as a common report by Murat Volkan Dülger. Therefore, the findings of this report are limited to the information obtained from the participants of meeting and the issues discussed during the meeting in relation to the subjects mentioned in the annexed agenda of the meeting.

The meeting was attended by fifty-one participants who are prosecutors from various provinces of Turkey working in cybercrimes and the regional court of appeals judges, Court of Cassation judges and prosecutors, police officers, gendarmerie, from Directorate General of Criminal Affairs, Turkish Bank Association, Information Technology and Communication Authority and other stakeholders in addition to Council of Europe experts.

C. General Assessment of The Meeting

The findings can be gathered under four main headings:

1. Investigating Cyber Crimes and Obtaining and Using Digital Evidence

- All prosecutors, security forces and CoE consultants agree on the inadequacy of the Article 134 in CPC (*Search of computers, Computer programs and transcripts, copying and provisional seizure*).
- The evidence collected by the police can easily become unlawful. The procedures to be followed are not considered in practice.

- The excessive workload at the stage of investigation (large increases in the number of investigation files in recent years) prevents an accurate and complete investigation.
- Capabilities and possibilities of police remain in the background, as the first statement is taken by the application prosecutor. This prevents asking the right questions to the victim, getting the right information from him/her and acting fast. Therefore, the first statement and contact should be done by the police, especially in cybercrimes.
- Communication and collaboration between institutions that gather information during the investigation phase should be facilitated. For example, making transactions through correspondence from banks extends the work a lot. Opening the banking system to UYAP is prohibited under the Banking Law. For this, a protocol can be made between the Ministry of Justice and the BDDK.
- Although there are thoughts on whether face recognition systems can be brought or not for the perpetrators who are withdrawing from the banks, it has been stated that these systems are very expensive and used only by the police for now. It is also thought that it may create a problematic field in terms of the law of personal data protection.
- Official expert cannot be found by the prosecutor for the cybercrime files, which are said to have not examined yet during the investigation process, or the police carry out the procedures too late due to the high workload. For this reason, when the prosecutor applies to the expert for a fee, it is seen that these experts are also police officers working in cybercrimes. Therefore, it is determined that they are sending files that should be examined as required by their duty to the experts by deliberately delaying. It seems that this has become a way of income and it is not true in the legal order.
- It may be legally appropriate to introduce the examination requirement as a prerequisite for litigation in cybercrimes like in tax crimes (tax crime report); it can be ensured that lawsuit is not be filed without this report.

2. Judgement of Cyber Crimes

- One of the most criticized issues is the lack of stability in the Court of Cassation's decisions and the lack of unity in the jurisprudence.
- The lack of specialization in courts of first instance is criticized. Because the evaluation and determination of especially the crimes in the articles of TCC 245/2,3, 245/A, 136 and 158 by the courts causes different criminal consequences.
- Illegal betting is one of the crimes that has increased tremendously in the last three years, and the security forces are sure that this crime is committed by organized manner. Therefore, regulations and measures must be prepared accordingly.
- In some crimes, the interval between the penalty for these crimes and the amount of punishment to be given should change. Legal regulations which were made regardless of the content of unjust, are subject to criticism.
- Due to the diversity and subjectivity of the violation of privacy issues, there are problems in ensuring legal security and unity in practice.

3. The Effect of Data Protection on Fighting with Cyber Crimes

- The number of committed cyber fraud crimes is increasing day by day according to published Interpol statistics.
- The widespread use of cloud computing tools and services brought major problems with regard to obtaining and dissemination of personal data unlawfully.
- Lack of awareness of victims about the importance of their personal data and the need to protect them leads to an increase in the number of crimes.
- Law No. 6698 Protection of Personal Data is not compatible with TCC.

4. Sexual Offences Committed Through Internet

- In child pornography, it is seen that children share child pornography especially on Whatsapp.
- Security forces are told that they are better than many countries' security forces on Deepweb.
- It is considered necessary to establish a relationship between TCC article 226/3 obscenity crime and article 103 sexual abuse crime. The lack of direct regulation of child pornography is a deficiency.
- It seems that the definitions of online sexual abuse crimes do not fully reflect CoE standards in this regard in domestic law.
- It is observed that there is a large lack of information about the presence of the 24/7 communication point working under the European Cyber Crimes Convention (Budapest Convention) before the General Directorate of Security, its duties and how it can help in investigations.

D. RECOMMENDATIONS

It is possible to gather the recommendations under the same headings just like the findings categorized above:

1. Investigating Cyber Crimes and Obtaining and Using Digital Evidence

1.1. The police should have a "checklist" of what to do when they encounter cybercrimes and what should be done at the most basic level should not be overlooked.

1.2. When to open to access certain digital evidence to the suspect/defendant and his/her defense counsel and the way they are collected is very important. The road map should be determined and applied strictly to collect legal evidence. Protocol/check list for police regarding handling electronic evidence and disclosing same to the accused and his/her lawyer could be considered.

1.3. Catalog crimes should be issued as soon as possible for CPC article 134 and it should be brought into compliance with the Budapest Convention. This needs to be taken into account in the arrangement, since the evidence collection for each crime has different characteristics.

1.4. In order to solve the heavy workload problems, it is necessary to carry out the projects for the law enforcement officers and the personnel responsible for the judicial stage, which trains people and to increase the capacity in the judiciary.

1.5. Since cybercrime prosecution offices are similarly under heavy workload, the prosecutors and assistant staff (clerks) working in this unit should be increased numerically, and all the staff working in this unit should also benefit from a technical informatics training program.

1.6. In addition to having experts in the field of fighting against these crimes and the incentive of the state to these professions will also have positive results.

1.7. Strengthening the institutions such as police cybercrime units with technical infrastructure services should also be considered as the top priority.

1.8. Communication and collaboration between institutions that will gather information during the investigation phase should be facilitated. At this point, especially the Turkish Banks Association and the Ministry of Justice should cooperate.

1.9. Training should be given to judges and prosecutors by expert bankers. Information on the introduce of banking products and services and the identification of known crime types should be shared. It will be useful to share the support and information expected from banks in judicial processes. With these trainings, improvement can be achieved in reaching the instant information needed.

1.10. Public / Private sector cooperation should be encouraged. In order to facilitate to obtain information by prosecutor from banks can be made to be in contact with "Fraud Prevention Working Group, the Banks Association of Turkey".

1.11. It is observed that there is a large lack of information about the presence of the 24/7 communication point working under the European Cyber Crimes Convention (Budapest Convention) before the General Directorate of Security, its duties and how it can help in investigations. In order to eliminate this, it is necessary to inform public prosecutors. There should also be a memorandum of cooperation between cybercrime prosecution bureaus and police.

2. Judgement of Cyber Crimes

2.1. Information on the detection of information crime types should also be shared in detail among institutions (Turkish Banks Association, Department of Cybercrime of Turkish National Police, relevant departments of gendarmerie and prosecution office).

2.2. It must be clearly demonstrated who owns the ownership and use rights of both, and who has the damage for the determination of the perpetrator in the crimes committed in cloud computing, when the action was against the information system, when it was against for the data contained in the information system or when this data was carried out against both the information system and the data.

2.3. At regular intervals, information sharing should be provided by holding meetings between judges and prosecutors, and even law enforcement officers who prosecute cybercrime.
2.4. Sanctions need to be diversified and determined.
2.5. In order to balance the file load in the criminal proceedings and to give the necessary importance to serious matters, like the practices in Europe, insults and libel crimes should be taken as a legal compensation instead of criminal proceedings, and these actions should not be criminalized.
2.6. It is of great benefit to establish a specialized court in the form of "IT courts" specializing in cybercrime and personal data.

3. The Effect of Data Protection on Fighting with Cyber Crimes

3.1. Planning education programs in schools will have positive results, especially in order to inform young people and adolescents about their personal data.
3.2. Training on personal data should be foreseen for all staff working in private or public institutions and organizations, as well as training modules proposed in the judiciary and law enforcement. Legal and criminal responsibilities of individuals should be informed with this training.
3.3. Even if it is an investigation carries out by the government, the use of personal data from data pools should be prevented, and there should be strict implementation in terms of protection and consent from individuals.
3.4. Even judges and prosecutors are making themselves insecure about the data and this should be prevented with training on data protection.

4. Sexual Offences Committed Through Internet

4.1. In the fight against cybercrimes, especially in sensitive issues related to children, the international authority problem should be solved, and the cooperation should be strengthened in the prosecution of these crimes within the framework of international cooperation due to the nature of these crimes.
4.2. In accordance with the opinion of the Lanzarote Commission, child pornography should be considered as a separate crime, and the legal regulations should be made to cover situations where the abuse occurred online beyond the meeting in person. In June 2015 the Lanzarote Committee invited states to extend the criminalisation of grooming also to cases when the sexual abuse is not the result of a meeting in person, but is committed online.
4.3. For a clearer and direct intervention, it is necessary to establish a relationship between TCC article 226 and article 103.
4.4. During the criminal proceedings of these crimes against children, the procedures and principles for the protection of witnesses and victims should be determined and implemented.
4.5. Another issue occurs while obtaining materials containing child pornography as evidence. Problems arising with the application of Turkish Criminal Procedural Code Act.134 should also be eliminated.

4.6. Country-specific materials can be developed and turned into a practice guide in cases of online child abuse by adding analysis of jurisprudence of ECtHR to ensure that domestic law is interpreted in the light of CoE standards.
4.7. Parents and caregivers should be informed and educated in general about IT crimes, and in particular for children they must be thoroughly educated.

5. Concrete Recommendations

In this section, in the light of the above findings, my suggestions for concrete outputs that can be made within the scope of the project are included.

5.1. There seems to be a major training gap in cybercrime and digital evidence. In order to eliminate this, training of trainers can be done. These people who are trained in the future can be provided with training in their own region.
5.2. Separate training modules can be prepared for the training of the trainers and for those attending the training.
5.3. After preparing modules and guides within the scope of this project, training activities can be carried out with the participation of all judges and prosecutors in various regions of the country.
5.4. One of the most important outputs of the project, which was completed in 2014, "Practice Guide" can be edited in the light of current developments and legislations. The guide itself and the correspondence samples included in the annex of the guide can be made available to all judges and prosecutors through UYAP. It may be one of the most important outputs of this project.
5.5. Update and adapt the CoE Electronic Evidence Guide into Turkish context and usage.
5.6. With the support of digital forensic experts (especially the police and forensic medicine experts), basic digital forensic information can be included in the training modules and application guide.
5.7. Amendments and the change demands to article 134 of the CPC can be proposed through a working group to be established under the project. This can be forwarded directly to the Ministry of Justice.
5.8. The checklist that was previously prepared and used to respond to IT crimes can be updated. This checklist can be made available to all judges and prosecutors via UYAP.
5.9. It can be provided to inform prosecutors working in the field of cybercrimes and prosecutors dealing with these crimes, about the 24/7 implementation of the police and preparing a brochure on this subject and for access on UYAP.
5.10. An information booklet on the protection of personal data in the context of GDPR and KVKK can be prepared and made available to UYAP for the use of all judges and prosecutors. In addition, training modules can be prepared by providing training on this subject.
5.11. By organizing a seminar together with the relevant departments of the Court of Cassation, efforts can be made to ensure the uniformity and harmony of the case-

law on IT crimes, the output of which can be made available as a booklet and accessible via UYAP.

5.12. Informative brochures on sexual abuse of children can be prepared and distributed to schools in cooperation with the Ministry of Education.

5.13. Workshops could be organised with a view of identifying specific gaps and challenges in domestic legislation and practice and ways of overcoming them (e.g. interpretation of domestic law under the light of CoE standards) in relation to online sexual abuse and exploitation of children. Moreover, the development of country specific material on relevant CoE standards that apply in Turkey could be useful. An in-depth analysis of caselaw of the ECtHR could also provide clear guidance as to the substantive and procedural obligations of judicial authorities when dealing with online sexual abuse of children cases. To this effect, a guidebook, check-lists or other practical material could be elaborated.

5.14. Need for a cybercrime prevention and education strategy, that will make the general public aware of the many dangers of cybercrime and also educate them. There is a need to arrange educational programme on cybercrime prevention and cyber security for children and teenagers. That Universities are encouraged to run and develop cybercrime prevention and cyber security courses so that in time Turkey will have a cyber educated workforce.

5.15. Online data protection course to be organized by judges and prosecutors;

5.16. Public / private cooperation to be encouraged. There was discussion on difficulties that prosecutors had getting information and data from banks, consideration should be given to making the “Working Group on the Prevention of Fraud, the Banks Association of Turkey” the contact point for prosecutors wishing to obtain information from banks. There should be a memorandum of cooperation among bank union, prosecutions service and police.

5.17. There should be a memorandum of cooperation between cybercrime prosecution bureaus and police. Coordination meetings could also be organized under the project could help to ensure focal points.

ANNEX : AGENDA OF THE MEETING

26 February 2020	Grand Efes 2
Wednesday	Hall

09.00 Registration

09.30 **Opening Speeches**

Elena Jovanovska-Brezoska, *Project Coordinator, Human Rights National Implementation Division, Council of Europe*

Kamil Erkut Güre, *Chief Public Prosecutor, Izmir*

Şenol Taş, *Deputy General Director of Criminal Affairs, Ministry of Justice*

09.45 **Keynote speeches**

Major Challenges in Fight Against Cybercrime and Crimes committed Online, Turkish Criminal Legislation and Good Practices

Mahmut Kaan Yüksel, *Public Prosecutor, Ankara*

10.15 *Coffee Break*

10.45 **First Session: Assessment and Admissibility of Electronic evidences – Good Practice and Challenges**

Chair: Assoc. Prof. Hasan Sınar, *National Consultant, Council of Europe*

Speakers:

Esther George*, International Consultant, Council of Europe*

Assoc. Prof. Murat Volkan Dülger, *National Consultant, Council of Europe*

Furkan Yılmaz, *Chief Inspector, Ankara General Directorate of Turkish National Police*

Ahmet Gül, *Public Prosecutor, Court of Cassation*

12.00 Discussion, Question – Answer

12.30 *Lunch*

26 February 2020	Grand Efes 2
Wednesday	Hall

13.30 **Second Session: Fraud on Internet**

Chair: Assoc. Prof. Murat Volkan Dülger, *National Consultant, Council of Europe*

Speakers:

Assoc. Prof. Hasan Sınar, *National Consultant, Council of Europe*

Fatma Aydın Khalil, *Chair of the Working Group on the Prevention of Fraud, The Banks Association of Turkey*

Erden Şahin, *Chief of Police, Ankara General Directorate of Turkish National Police, Investigation Department*

14.30 Discussion, Question – Answer

15.00 *Coffee Break*

15.20 **Third Session: Online sexual exploitation and abuse of children (International standards, national practices, challenges for investigations)**

Chair: Assoc. Prof. Hasan Sınar, *National Consultant, Council of Europe*

Speakers:

Dr. Maria Andriani Kostopoulou, *International Consultant, Council of Europe*

Prof. Veli Özer Özbek, *National Consultant, Council of Europe*

Adem Can, *Public Prosecutor, Ankara*

16.20 Discussion, Question – Answer

17:00 **End of the First Day**

27 February 2020	Grand Efes 2
Thursday	Hall

09.30 **Fourth Session: Protection of Personal Data while Fighting Cybercrime**

Chair: Assoc. Prof. Murat Volkan Dülger, *National Consultant, Council of Europe*

Speakers:

Esther George, *International Consultant, Council of Europe*

Assoc. Prof. Hasan Sınar, *National Consultant, Council of Europe*

Mahmut Esat Yıldırım, *Cyber Security Expert, Information and Communication Technologies Authority, Information Technologies Department*

10.45 *Coffee Break*

11.00 Discussion, Question – Answer

12:00 **Recommendations for further developments**

Assoc. Prof. Volkan Dülger, *National Consultant, Council of Europe*

12.45 **Closing remarks**

Şenol Taş, *Deputy General Director of Criminal Affairs, Ministry of Justice*

13.00 *Lunch*

14.00 **End of the programme**