Legal Reflections on 24/7 Point of Contact and Preservation Requests

Workshop Report

TURKISH NATIONAL POLICE
DEPARTMENT OF CYBERCRIME

Contents

1 Introduction 3
2 Discussion of questions and scenarios 6
2.1 Question 1 - Immediate Assistance 6
2.2 Question 2 - Categories of data 7
2.3 Question 3 – Authorising the National 24/7 Point of Contact to share information outside the context of a criminal investigation 9
2.4 Question 4 - Criminal responsibility for sharing information 10
2.5 Question 5 – Responsibility for failure to share information 11
2.6 Question 6 – Sharing information on foreign nationals and citizens 13
2.7 Question 7 – Liability for notification 14
2.8 Question 8 – Liability for deletion of data 16
2.9 Question 9 – Liability of company managers 17
2.10 Question 10 – Refusal to cooperate 18
2.11 Question 11 – Suspension of suspicious transactions 19
2.12 Question 12 – The power of LEA to suspend bank accounts 21
2.13 Question 13 – The requirement of having statements from foreign victims in cases of fraud 22
2.14 Question 14 – Use of data after retention period expires 23
2.15 Question 15 – Real-time collection and partial disclosure of traffic data 25
2.16 Question 16 – Real-time interception of content data 26
2.17 Question 17 – Spontaneous information 28
2.18 Question 18 – Sharing information through e-mails and direct co-operation with ISPs 30
3 Conclusion 32
4 List of participants 33

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe, the donor funding iPROCEEDS project or Parties to the Budapest Convention on Cybercrime.

1 Introduction

The Council of Europe Convention on Cybercrime (Convention) was signed in Budapest, Hungary in 2001. It is the first international treaty that has been prepared with regard to offences committed against and by means of computer systems, the main aims of the Convention are to ensure consistency among countries in the definition of cybercrimes in the criminal laws, put in place procedural measures that would allow expedited access to digital evidence, as well as ensure effective international cooperation in combatting cybercrime and sharing of information.

More than 60 countries, including the United States and Japan, which are not members of the Council of Europe, are parties to the Convention. Moreover, certain countries that are not signatories of the Convention have shaped their legal framework by using definitions of cybercrime offences and other measures provided in the Convention. Turkey signed the Convention on 10 November 2010; the Grand National Assembly of Turkey ratified it on 22 April 2014 after discussing it in the Plenary Session. The Convention entered into force on 2 May 2014 with the publication of Law no. 6533 on the Approval of the Convention on Cybercrime in the Official Gazette.

Contrary to physical evidence that is subject of the investigation of conventional crimes, digital data is volatile and failure to implement legal measures for their expedited preservation may hinder criminal investigations. In order to ensure the provision of digital evidence requested through mutual legal assistance proceedings, which usually lasts for months, the Convention provides for "preservation requests" in Articles 29 and 30. The 24/7 national points of contact, designated as per Article 35 of the Convention, hand in the preservation requests to the relevant service providers and the service providers submit digital data to the judicial authorities of the requesting state upon receiving the letter rogatory. The Cybercrime Department of the Turkish National Police assumes the role of the National Point of Contact on behalf of Turkey on a 24/7 basis. In addition to dealing with data preservation requests and requests for information in emergency cases, it provides technical and legal assistance on issues related to criminal investigations to the requesting states.

The National 24/7 Point of Contact is one of the international police cooperation channels and due to its nature may only be used in emergency cases. Law enforcement agencies use Interpol and Europol channels frequently; exchange of information and experience takes place face-to-face through liaison officers of foreign law enforcement agencies. The assistance currently provided through the National 24/7 Point of Contact only constitutes a small percentage of the entire international police cooperation. The main reason for the small number of preservation requests received by Turkey could be attributed to the low number of Turkey-based service providers

used by foreigners and hence, relatively low number of foreign victims. On the contrary, the low number of preservation requests sent by Turkey is a result of the lack of information concerning the functions of the National 24/7 Point of Contact.

The Council of Europe Cybercrime Convention Committee (T-CY) observed similar problems in other countries and has adopted a recommendation for the authorities, namely that the 24/7 National Point of Contact needs to be introduced to other stakeholders in the country more effectively.[1]

Turkey has undertaken work regarding harmonisation of its substantive and procedural criminal law with the provisions of the Convention. However, no regulation has been made with regard to the functions of the National 24/7 Point of Contact, primarily in relation to data preservation requests and expedited international sharing of information. So far, the 24/7 National Point of Contact used the power granted by legislation to deal with the preservation requests and other urgent requests without contradicting domestic law. Nonetheless, the lack of detailed regulations and differences that exist in the national legislation related to service providers and the provisions on corporate liability contained in the Convention, sometimes cause drawbacks in implementation.

In order to increase awareness of the national stakeholders on the National 24/7 Point of Contact and create intellectual resources for future harmonisation of the Turkish law with the Convention; judges, prosecutors, officials of the Ministry of Justice, access providers and hosting service providers, as well as representatives of academia have been invited to the workshop "Legal Reflections on 24/7 Point of Contact and Preservation Requests" that was held in Istanbul on 15-16 April 2019. The meeting was partially funded by the Joint Project of the European Union and the Council of Europe on targeting crime proceeds on the Internet in South Eastern Europe and Turkey - iPROCEEDS.[2]

Before the event, 18 questions and scenarios were disseminated to participants who had to reflect and compile answers. These were prepared based on the vast experience of the National 24/7 Point of Contact and at the same time, reflect the current developments related to combatting cybercrime discussed worldwide. The unofficial Turkish translation of the Convention's Explanatory Report has been sent to participants.

On the first day of the workshop, the 24/7 Points of Contact of France, Latvia and Romania have made presentations. They also received the questions and scenarios but of a more general nature, excluding the parts related to the Turkish legal system. The responses of the foreign 24/7 Points of Contact have also been summarised in this report, where applicable, and included under

1 *See* Recommendation 5, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 2014, p. 125, https://rm.coe.int/t-cy-2017-18-opinion-article29-/168076cf95

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

the relevant responses. During the remaining part of the event, national participants have held discussions divided in five groups within the timeframe granted to them by the moderator. Then, the views and opposing views of the groups have been discussed. Discussions were recorded electronically and have been compiled in this report by anonymising them and by maintaining a critical balance between the whole text and presenting all the ideas. Needless to say, in case there are contradictions between the Budapest Convention and its explanatory notes and the legal interpretations of Turkish experts, the former must be taken as the primary source of information.

Also, for the purposes of this workshop, the National 24/7 Point of Contact officials have used the Tallinn Manual on the International Law Applicable to Cyber Operations that enlists the possible rules of international law that could be applied in NATO's stance in relation to cyber conflicts and cyber warfare.

The results of the workshop are published in Turkish and English as on online open source. It aims to contribute to the discussions of National 24/7 Points of Contact from other countries that are engaged in similar efforts and inspire academic discussions and potential legislative changes in Turkey.

As officials of the National 24/7 Point of Contact, we would like to express our gratitude to Mr. Erdal ÇETİNKAYA, Head of the Department of Cybercrime of the Turkish National Police, who has never refrained from giving utmost moral and material support for the implementation of this workshop, to the iPROCEEDS project, and to our valuable participants who have contributed greatly to this report with their precious ideas based on their unique experiences.

2 Discussion of questions and scenarios

2.1 Question 1 - Immediate Assistance

Please discuss the scope of the concept of "Immediate Assistance" provided in Article 35 of the Council of Europe Convention on Cybercrime (hereinafter, Convention) in the context of Turkish legal framework and universal legal principles.

- **Should this concept cover only close imminent threats to the life or physical integrity of individuals?**
- **Should it also cover the instances of threat to wealth, property or critical digital data infrastructure? Please express your expert opinion with reference to examples.**

The moderator has started the session by generally informing that the Convention has formal and informal channels of communication. This also includes the 24/7 Points of Contact Network for exchange of information between domestic law enforcement officers within the scope of international police cooperation. Also, it was noted that Interpol communication system is used most frequently by the states.

The participants have reached a consensus that imminent threat to human life or to the physical integrity of individuals should be considered in the context of "immediate assistance" and that this concept, which has not been able to find a place within the Turkish law, should be expressly regulated.

However, different legal interpretations have emerged for the situations remaining outside this matter. Certain participants, referring to the text of the Convention and its Explanatory Report, have claimed that the "immediate assistance" concept of the Convention could be applied to all criminal offences, for which digital evidence exists, since it is a concept related to procedural provisions.

Yet, some participants have pointed out that such a broad interpretation could cause a contradiction with the provisions related to personal data provided in Articles 135 and 136 of the Turkish Penal Code. In this respect, they have emphasised that each request received by the National Point of Contact should be considered in view of personal rights. This tool should not be resorted to in cases where individual interests override public interests.

Also by referring to the concept of "the emergence of damages that are difficult or impossible to remedy" within the Turkish law, many participants have claimed that accessibility

to digital data could easily be eliminated and therefore, the scope of immediate assistance could be expanded to cover other offences, including those against property, computer-related offences against critical infrastructure and online child abuse. Lastly, one participant has conveyed his view that the concept of "immediate assistance" has been completely misinterpreted and that what is really meant in the Convention is "instant assistance". In this context, it has been claimed that the rapid and effective assistance provided by the National 24/7 Point of Contact to the requesting state has been defined irrespective of the nature of the offence subject to the request.

The Latvian National Point of Contact official has noted that terrorist attack threats and cases where the safety of persons' lives is in danger are considered as states of emergencies.

Important Note: Not every request sent to the National 24/7 Point of Contact from other countries may require the initiation of a legal investigation in Turkey. When responding to the following questions, please take into consideration the options of the Public Prosecutor to both initiate and not initiate/ not being able to initiate an investigation.

2.2 Question 2 - Categories of data

The Turkish National Point of Contact forwards without delay the request of the country A for immediate assistance to the relevant Internet Service Provider. The request covers subscriber information, all traffic data and all content data of a user on a website. Considering that subscriber information does not have a clear definition in our domestic law, please give your expert opinion on the conceptual discussions and potential scenarios below.

- **What kind of data do you think subscriber information should contain and what kind of legal regulation should it be delimited by?**
- **Some Internet Service Providers store the last 50/100 IP addresses that access a user's account (last login IPs) as subscriber information. Do you think the Turkish legal framework permits a similar practice?**
- **There is no reference to content data in our domestic law. Do you think that Turkish legal framework should provide for this gap?**
- **Please discuss through concrete examples the legal requirement for the aforementioned classification or whether it is necessary to provide definitions of data in full compliance with the Convention.**

The moderator started the session by explaining the concept of last login IPs. Websites store the data on the IP addresses by which their users log in. When the identity details of a user are requested the foreign Internet Service Providers send to the law enforcement unit 10 to 100 IP addresses and their access times related timestamps. As the relevant user only had access to a certain website at a certain period of time, this information is not enough to access any other personal information. The rationale of this practice is that once an IP address and an access time are obtained, it is not possible to identify a user who uses a VPN (Virtual Private Network) or who is assigned a NAT IP (Network Address Translation) by the Internet Service Provider. Having multiple connection data is very important for reaching and authenticating the true identity of the relevant user.

Although many participants pointed to a detailed definition of the subscriber information stipulated in Article 18 of the Convention, no consensus has been reached on the scope of subscriber information. However, all participants have agreed that this drawback should be remedied through legislative regulation. Most of the participants indicated that an amendment should be introduced in Law no. 5651 on "Publications on the Internet and Combating Crimes Committed by Means of Such Publication" or a regulation that would explain the relevant definition indicated in this Law. One participant has commented that the definition of "subscriber's identity and communication data" stipulated in the Law no. 5809 on "Electronic Communications" could be extended. Also, one participant has emphasised that the Convention clearly indicates that subscriber information is different from traffic data and that in terms of procedural law, has adopted a "production order" for subscriber information and a "preservation order" for traffic data.

It has been claimed that in order to avoid problems in cooperation with the parties to the Convention, the term subscriber information should be removed from the definition of traffic data in Law no. 5651. According to the participants, it is acceptable to have last login IPs as mentioned above, if user's privacy is not violated by disclosing the Internet browsing history for profiling purposes.

Agreeing on the lack of a legislative regulation regarding the scope of content data, participants have made different suggestions. It has been emphasised that by updating and using a common terminology in one or more laws, including Law no. 5651 on "Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication", Law no. 5809 "Electronic Communications" or Law no. 6698 on "the Protection of Personal Data", drawbacks in implementation and potential instances of unfair treatment could be prevented.

While Law no. 5651 brings clear rules regarding the liabilities of service providers for storing traffic data, some participants have noted that a considerable gap exists when it comes to the legal liabilities of content providers and content data. They have pointed out that it is necessary to establish a legal framework to ensure accessibility to digital evidence during investigation and

prosecution and to determine legal and criminal liabilities of content providers based on objective criteria.

In addition, one participant has made an interesting point about the concept of content data in the Turkish law. The incoherence existing in theory and in practice was exemplified by referring to Law no. 5651 that covers the content provided via internet, Law no. 5809 that regulates the content data occurring between two computer systems but not being published on the internet, and Article 135 of the Turkish Criminal Procedure Law, which refers to the content data concerning the communication between two individuals.

2.3 Question 3 – Authorising the National 24/7 Point of Contact to share information outside the context of a criminal investigation

According to the additional Article 6 of the Law on Police Duties and Powers, "As regards the cybercrimes, the police shall be authorised to have access to identity information of the internet subscribers and to conduct cyber inquiries with a view to establishing the competent Chief Public Prosecutor's Office in that regard. Access providers, host providers and content providers shall communicate the requested information to the relevant police unit established for the purpose of fighting against such crimes".

- **If there is an information request that cannot be made a subject of a criminal investigation in Turkey, is it possible for the National Point of Contact to share information directly based on the aforementioned article?**
- **If no, what amendments should be made to give such power to the National Point of Contact?**

Pointing out that the additional Article 6 of the Law on Police Duties and Powers allows police requesting subscriber information just for the purpose of identifying the competent Public Prosecutor's Office, the majority of the participants have said that it would not be possible to exercise this authority in the absence of a Public Prosecutor.

While some participants stated that it was necessary to discuss the power of sharing information outside the context of a criminal investigation, others stated that it was possible to give the power to share information with certain restrictions through legal regulations and international treaties. Since some participants have questioned the compatibility of the said provision with the Turkish legal system, one participant has explained in detail why such power has been granted

to the law enforcement officers. The reports submitted particularly by the non-governmental organisation, the National Centre for Missing and Exploited Children (NCMEC) in the United States, on the users who have uploaded child abuse materials onto the platforms of Internet Service Providers, such as Facebook, Google and Twitter, are first submitted to the Department of Cybercrime, and then to the Public Prosecution Office of the relevant provinces. Before granting authorisation to law enforcement authorities to directly request subscriber information, most of the reports focused on certain provinces. However, when the Public Prosecution Office identified the location, it was found that many users actually resided in other provinces. For such reasons, sometimes it took up to two years to reach some of the suspects. Lawmakers have authorised the law enforcement agencies to directly request subscriber information in order to access digital data more quickly and store data efficiently, significantly shortening the process detailed above.

Some participants have pointed out that it is necessary to discuss the issue of authorising the National 24/7 Point of Contact to share detailed information outside the context of a criminal investigation, others have said that only limited sharing of information could be allowed through legislative regulations or agreements concluded between states.

2.4 Question 4 - Criminal responsibility for sharing information

According to the Article 90 of the Constitution of the Republic of Turkey "International agreements duly put into effect have the force of law. In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail". Based on this Article, although there is no clearly stated obligation in domestic law, the Internet Service Provider submits the necessary information to the National Point of Contact. However, later on, the Public Prosecutor initiates a criminal investigation against the National Point of Contact and the Internet Service Provider on grounds that they have performed an illegal action.

- **In the aforementioned case, do the National Point of Contact and the Internet Service Provider bear criminal liability pursuant to the Turkish Penal Code?**
- **If yes, please explain in detail the source of criminal liability and in which legal documents amendments must be made to remove this responsibility. If no, please explain the reason why the action taken is lawful.**

Despite hesitations of several participants, most of the participants have agreed that the Convention indisputably relates to fundamental human rights and freedoms and therefore, is a binding text above the laws in the Turkish legal system. The Convention is closely affecting the right to privacy and freedom of expression through the procedural measures, such as search, seizure and interception of communication in real-time, has been presented as a supporting argument. Therefore, it has been indicated that even though there is no expressly defined authorisation or responsibility in domestic law, the Internet Service Providers that provide subscriber information to the National 24/7 Point of Contact shall not bear any criminal liability for not implementing Article 18 of the Convention. In this case, it was emphasised that the reason for compliance with the law stated in Article 24 of the Turkish Penal Code, that is "carrying out the provisions of a statute", would be fulfilled.

As regards the possibility of National 24/7 Point of Contact to share information with the Points of Contact of other countries, the participants have reached a consensus on the issue that the same reason for compliance with the law shall emerge for instances that could be subject to a criminal investigation in Turkey. Although the Convention does not require double criminality for international cooperation, some participants have said that a legislative regulation is necessary in order for the National 24/7 Point of Contact to share information with other countries' Points of Contact in cases where a criminal investigation is not/cannot be initiated in Turkey.

One participant has noted that according to Article 8 of the Law no. 6698, personal data cannot be transferred without explicit consent of the data subject and that exceptions to this rule have also been listed in the same article. In this respect, the participant has underlined that the National 24/7 Point of Contact and the Internet Service Provider would face criminal responsibility for sharing information unlawfully, subsequently legislation regulating sharing information at international level by the National Point of Contact is necessary to prevent this.

2.5 Question 5 – Responsibility for failure to share information

Since there is no clearly stipulated rule in domestic law, the Internet Service Provider refrains from sharing information directly with the National Point of Contact and requests for a prosecutor or a court order. However, judicial bodies state that the request could only be processed if it is based on a mutual legal assistance request received diplomatic channel. Meanwhile, the offense takes place in country A and material damage, harm or loss occurs as a result.

- **In terms of national and international law, could it be claimed that an individual or**

institution has legal liability for the offense that takes place in country A?

- **In the case above, would it be possible for judicial authorities to refuse to process the request for information by issuing a lack of jurisdiction decision?**

The divergence of views among participants as to the role of the Convention within the Turkish legal system has also emerged in the answer to this question. Some participants have argued that the Internet Service Provider would have legal liability for failing to fulfil the provisions of the law. It has been pointed out that regardless of the damage that took place in country A, both the service provider and the Public Prosecutor could be charged with neglect of duty and/or misconduct. Whereas, one participant, by referring to the 2001 of the United Nations' International Law Commission "Draft Articles on Responsibility of States for Internationally Wrongful Acts" has noted that the gross and systematic failure to fulfil an international obligation is defined as a serious breach and that states could also be held responsible in that respect. On the other hand, some participants have said that the relevant individuals and organisations cannot be held criminally responsible unless the liabilities included in the Convention are supported with legislative regulations in domestic law. In addition, one participant has conveyed that the rules and procedures applicable to Turkish citizens were also binding for the requests made to the National Point of Contact since there was no legal provision expressly stating the contrary.

A consensus has also been reached on the fact that it might be impossible for judicial authorities to respond legally to a request received by the National 24/7 Point of Contact by issuing a decision of lack of jurisdiction. One participant has reminded that a lawsuit would be filed in a court of jurisdiction according to Turkey's judicial system, emphasising the importance of authorisation. The same participant has also commented that for resolving potential problems that exist in practice related to authorisation, establishing a judicial body that has jurisdiction all across Turkey for processing the requests received by the National 24/7 Point of Contact would be the most ideal solution.

The Latvian National 24/7 Point of Contact official has noted that in such a situation, the offense of "Failure to Fulfil the Legal Requests of the Supervisory or Local Government Body Officials" defined in paragraph 2 of Article 175 of the "Administrative Violations Law" would emerge, and that the relevant Internet Service Provider would have legal liability.

2.6 Question 6 – Sharing information on foreign nationals and citizens

This time, the judicial authorities issue the order requested by the Internet Service Provider. The concerning suspect is a foreign national living in our country. Could information that belongs to a foreign national be shared with the authorities of another country?

- **If your answer is yes, what are the restrictions of this sharing?**
- **If the suspect is a citizen of the Republic of Turkey, would there be any difference in the rules and procedures that must be followed?**

Please share your opinions and suggestions on the determination of procedures and principles depending on the type of the data requested (subscriber information, traffic data, content data) to be shared with other National Points of Contact.

All the participants have stated that, based on the principle of territorial jurisdiction as referred to in Article 8 of the Turkish Penal Code, there would be no difference in sharing of information concerning foreign nationals in Turkey and Turkish citizens. Some participants have referred to conditions of special status, such as diplomatic immunity, which constitutes an exception, and to the possible applications of the provision, "the fundamental rights and freedoms of aliens may be restricted by law in accordance with the international law", as stipulated in Article 16 of the Constitution.

The lack of a legal provision in the domestic law regarding international sharing of information by the National 24/7 Point of Contact has been pointed out once again. The participants have also agreed that it is necessary to make a legal distinction regarding sharing of information depending on the type of data requested.

The National 24/7 Point of Contact officials of France and Latvia have indicated that no special regulation has been introduced that refers to sharing of information regarding foreign nationals with other Points of Contact. The officials have also provided details on sharing information in their country as part of international police cooperation. The National 24/7 Point of Contact of France has noted that in cases that do not require an investigation to be opened, more extensive cooperation could be established with the country requesting information. Whereas, the National 24/7 Point of Contact of Latvia has said that the natural limits of sharing information with other countries are determined by the provisions of the Constitution of Latvia, the concept of state sovereignty, and to the extent that no obstacles are created for local investigations.

2.7 Question 7 – Liability for notification

Country A issues a data preservation request to the National Point of Contact related to the online grooming of a child living in their own country. The Point of Contact requests the Internet Service Provider not to inform the suspect about this. Due to the company transparency policy and the lack of clear regulations in the national legal framework that would prohibit notification in certain cases, the ISP notifies the suspect of the preservation request. Now being aware of the investigation in country A, the suspect deletes all digital material on the devices. When a letter rogatory is received from country A and the person's computer and mobile phone are examined; no evidence can be found that shows that this person attempted to groom children online who live abroad.

- **In this case, does the Internet service provider have any legal, administrative and criminal liability?**
- **If your answer is yes, what kind of sanctions could be imposed?**
- **If your answer is no, what kind of regulations could be adapted in order to hold the Internet service provider liable to notify in similar cases?**

Participants have said that in the case of a request for information that may be the subject of an investigation in Turkey, the Internet Service Provider that informed the suspect despite the National 24/7 Point of Contact's instruction to the contrary, shall be held criminally liable. Reference has been made to paragraph 2 of Article 285 of the Turkish Penal Code that states: "Any person who breaches the confidentiality of decisions and subsequent actions carried out pursuant to these decisions, which are taken at the investigation stage or required to be kept confidential in respect of those who are party to the investigation, shall be sentenced to a penalty of imprisonment for a term of one to three years and judicial fine".

Since the Turkish Penal Code does not stipulate any criminal liability for legal entities, it has been concluded that the employees of the relevant unit of the Internet Service Provider could be penalised under this article. Noting that this provision would be an insufficient sanction in the face of fatal consequences that could emerge, some participants have conveyed that it would be more appropriate to subject Internet Service Providers to a more severe penal sanctioning as an independent type of offense in cases of infringing the non-notification request in criminal investigations. In such a case, comments have been made that administrative fines would be more deterrent for institutions.

It has been suggested that severe administrative fines could be imposed with regard to the

violation of the data controller's obligation to safeguard data under Article 12 of Law no. 6698 and the violation of the hosting provider's and access provider's obligation to store data under Law no. 5651. In identifying the legal liability of the Internet Service Provider, participants have drawn attention to the challenges in the determination of the tangible and intangible damages in the abovementioned case, as well as in connecting this damage to the obligation of not notifying against the order and have refrained from making any clear comments.

It has also been stated that in circumstances where a criminal investigation is not/cannot be initiated in Turkey, the Internet Service Provider could be subject to criminal liability according to the general provisions stipulated in the Turkish Penal Code, such as neglect of duty or misconduct. Some participants have argued that administrative fines could even be imposed in such cases.

However, by referring to Law no. 5651 item d of paragraph 1 of Article 6, which was repealed by the Constitutional Court, one participant has stated that this procedure cannot be applied. This article provides that Internet Service Providers are obligated to submit the information requested by the Information and Communication Technologies Authority in the required form and to implement the measures requested by the Authority. In its decision of 8 December 2015, the Constitutional Court has concluded that personal data could also be included among the requested information and therefore, the concerned persons must be informed. It has been conveyed that for this reason, the Internet Service Provider cannot be held administratively responsible in the absence of an obligation to notify expressed clearly in the law, such as not breaching the confidentiality of an investigation.

The National 24/7 Point of Contact of France has stated that a similar case has not yet been experienced in their country in the light of good cooperation with the Internet Service Providers. The Point of Contact has also said that they received feedback from service providers indicating that the liability of not notifying was in compliance with the European Union General Data Protection Regulations (GDPR). Furthermore, it was indicated that in the event of a service provider wanting to notify the concerning person, the Point of Contact of the requesting country would be informed about this situation and the process would take shape according to the request of that country. It has also been conveyed that if there is no criminal investigation being carried out in France, the service provider shall not have any legal responsibility even if it notifies the concerned user.

On the other hand, the National 24/7 Point of Contact of Latvia has pointed out that the service providers are also responsible for the preservation of data that they process pursuant to the Code of Criminal Procedure of Latvia and that criminal liability could arise in case of sharing information that must be kept confidential.

2.8 Question 8 – Liability for deletion of data

Country A issues a data preservation request to the National Point of Contact of another country. Following the necessary procedures, the Internet Service Provider initially accepts to do whatever it is necessary in terms of the request and informs the Point of Contact that the relevant data are being preserved. However, when the letter rogatory reaches Turkey, it becomes evident that all the data have been permanently deleted.

- **In this situation, what is the administrative and/or criminal liability of the Internet Service Provider?**
- **In terms of legal liability, is there any difference between the data being deleted intentionally or negligently?**

In the case of an ongoing criminal investigation in Turkey related to the the request, the participants have reached a consensus that an administrative fine could be issued in terms of liabilities, as it violates administrative responsibility stipulated in the above-mentioned laws no. 6698 and 5651.

In terms of criminal liability, the applicability of Article 281 of the Turkish Penal Code has been discussed in relation to concealing, destroying and altering evidence of an offence. It has been concluded that the specific intention to "prevent the emergence of the truth", required by this article, cannot take place in practice or will not be possible to proven it, even if it takes place. It would not be possible to attribute criminal liability since Internet Service Providers usually automatically erase or destroy data and Article 281 of the Turkish Penal Code cannot be committed without intention. The participants have indicated that their answers to question 7 (paragraph 2) are also generally applicable to this scenario in case there is a criminal investigation being conducted in Turkey. The act of erasing data can only be penalised if it breaches the general provisions of the Turkish Penal Code or laws providing for administrative liabilities.

The National 24/7 Point of Contact of France has noted that the service providers in certain situations have erased data subject to preservation requests since the countries issuing a data preservation request have not sent letters rogatory. In such a situation, the service provider does not have any legal liability. The National 24/7 Point of Contact of Latvia has indicated that in cases where the service provider intentionally erases data, which it is obliged to preserve, the offense of "destroying evidence" shall be at stake according to the Penal Code of Latvia.

2.9 Question 9 – Liability of company managers

Article 12 of the Budapest Convention is related to the liability of legal persons. Assume that the request for data preservation is related to a computer on the network of a large company. The company manager officially notifies the National Point of Contact that they will do whatever is necessary to preserve data. However, the data is not available when needed.

- **According to the Turkish legal system, is there a difference between company managers and Internet Service Providers with respect to liabilities?**
- **If the company manager refuses to comply with the data preservation request, which legal procedures could the National Point of Contact resort to?**

The participants have indicated that the liability of legal persons provided in Article 12 of the Convention also applies to private law legal persons, other than service providers, who are held liable according to the Law no. 5651. They have also said that the retention of data, other than data related to Internet access, is usually left to the discretion of the departments of information technologies of legal persons. In case the National 24/7 Point of Contact is issuing a preservation request, the legal liability of the relevant company should be clearly defined.

Although the Law on the Protection of Personal Data provides for various liabilities for legal persons for the processing of data, the view that the relevant provisions may not be regarded as a legal foundation for fulfilling the data preservation request have been dominant. In addition, it has also been stated in the context of Article 12 of the Convention that making the necessary amendments in domestic law constitutes a pre-requisite for imposing any liability on a legal person.

Article 20 of the Turkish Penal Code illustrates the impossibility to attribute criminal liability to legal persons. They have also agreed that since the necessary liability has not been defined in the domestic law through regulation, the procedural measures stipulated in Article 133 of the Turkish Penal Code cannot be applied in case the company manager refuses to fulfil the data preservation request made by the National 24/7 Point of Contact. Therefore, it has been concluded that there is no legal remedy for obliging or ensuring that legal persons comply with a data preservation requests of the 24/7 National Point of Contact.

The National 24/7 Point of Contact of France has indicated that there is no difference between Internet Service Providers and company managers in terms of legal liability. Whereas, the National 24/7 Point of Contact of Latvia has stated that company managers are only responsible for the physical data held by the company.

2.10 Question 10 – Refusal to cooperate

The Turkish National Point of Contact issues an urgent request to country A concerning a potential terrorist attack. Although the National Point of Contact is publicly listed in the Directory of 24/7 Points of Contact of the Council of Europe, the authorities of country A claim that they could not validate the national point of contact and asks instead to issue the request through the Interpol communication channel that will require longer time. Meanwhile, the terrorist attack takes place and causes damages that are difficult or impossible to repair.

- **In a situation like this, will it be possible to initiate a legal or diplomatic procedure against the Point of Contact of another country?**
- **Assume that the Point of Contact of country A never responds or responds very late to the e-mails and phone calls that must be available on a 24/7 basis as stated in the Convention. Is it possible for a difference to exist in the legal approach to be taken in this scenario?**

The participants have emphasised that there would be no differences in the legal and diplomatic measures that could be taken against cases where the National 24/7 Point of Contact violates the obligation to respond quickly or does not respond at all. They have agreed that diplomatic means could mostly be resorted to in case a situation like that given in the scenario takes place. By referring to Article 45 of the Convention, the participants have expressed that in case of a dispute occurring between two member states, the matter could be referred to an arbitrator, the European Committee on Crime Problems or to the International Court of Justice. It has also been highlighted that even if by a very slight chance, the damages could be compensated in the context of legal liability, through determination of a connection between the damage occurred and the 24/7 Point of Contact's negligent behaviour, still there have been some hesitations as regards to whether application should be made to the judicial authorities of the country in which the damages occurred or to the judicial authorities of the foreign country.

The National 24/7 Points of Contact of France and Latvia have drawn attention to other channels of communication such as Interpol, Europol and embassies that could be used in such cases. They have also indicated that it is possible to resort to diplomatic means in the event of damages arising from an intentional act.

2.11 Question 11 – Suspension of suspicious transactions

A person who compromised the SWIFT system of a bank based in country A by sends the profits obtained from this offense to the bank accounts in Turkey. In order to prevent the money from being withdrawn from the account or being transferred to a third country, the Point of Contact of country A requests immediate suspension of the relevant bank account and the return of the money transferred. Please answer the following questions respectively.

- **In case of such a suspicious transaction, is it possible for the bank to suspend one of its accounts on its own initiative without a prosecutor or court order?**
- **If yes, what is the maximum period that it could suspend it for?**
- **Assume that the bank has temporary suspended the account for transactions until a court order is issued. Meanwhile, the owner of the account threatens the bank with launching a legal action in order to withdraw the money. Please examine thoroughly the powers and responsibilities of the bank towards the owner of the account and the person who reported the suspicious transaction.**
- **If the bank does not suspend the account by taking initiative and causes an irrecoverable financial loss for the foreign victims, is it possible to compensate the loss of the victims through legal means?**
- **In such cybercrime investigations, it is mostly difficult to gather all the evidences related to the illegal act at the initial stage as seen in the example. By reaching the conclusion that the aggrieved country does not have adequate evidence related to fraud, judicial authorities do not reach a decision or decide to lift the temporary suspension measure. What are the conditions and limits of restricting the exercise of a financial right according to the existing regulations of domestic law? If you think that these are not sufficient, please share your suggestions.**
- **Everything goes as planned and the bank suspends the account through a judicial ruling. However, the letter rogatory concerning the investigation does not reach Turkey. For how long should the bank wait before allowing the use of the account to? Do you think that the account should be reactivated on its own at the end of a certain period or should the account owner make a personal request?**

The participants have brought forth many legal bases for banks to suspend the accounts of persons when being informed of a suspicious transaction. They have emphasised that general

agreements concluded between banks and their customers contain articles that stipulate in which conditions the bank could directly suspend and close accounts and that in practice, banks usually act based on such contractual agreements.

For how long the accounts could be suspended by the bank also depends on the contract terms. These could be suspended for an indefinite period. It has also been stated that with Article 7 of Law no. 5549 on "Prevention of Laundering Proceeds of Crime", banks have the obligation to report suspicious transactions to the Financial Crimes Investigation Board (MASAK) and then suspend the relating accounts for a period of seven days. Apart from these, participants have also pointed out that bank accounts could be confiscated or its use by the account owner could be restricted within the scope of Article 128 of the Turkish Criminal Procedure Code no. 5271, Law no. 6415 on "Prevention of the Financing of Terrorism" and Banking Law no. 5411.

It has also been indicated that a person whose account has been suspended ex officio by the bank could resort to legal actions until a judicial ruling is issued. In the case of a third party who is not a party to a contract signed with the bank incurring a loss, the bank shall be held responsible for the entire account, which has not been suspended, as well as for the accrued interest and additional losses.

In practice, rather than assuming such a heavy responsibility, banks would prefer to suspend the relevant account and accept any responsibility arising from the inability of the holder to use that account for a certain period. The person whose account is suspended will be able to file a lawsuit seeking for damages in accordance with the provisions related to tortious acts provided in the Turkish Code of Obligations. However, many participants have emphasised that judicial authorities would rule in favour of the bank in case the bank accounts are used for illegal purposes and therefore, no legal and criminal liability would arise in practice in regard to account suspension.Similarly, foreign persons reporting the suspicious transaction to the National 24/7 Point of Contact and those who incur losses due to the bank not suspending the relevant account may also file a suit for damages.

The measure of suspending the relevant bank account could be revoked with a court decision and it is not possible for the bank to challenge such a decision through legal means. Moreover, in such cases, the decision should be executed without requiring the application of the account owner and the account must be reactivated immediately. Whereas, in cases of the measure not being revoked through a court decision, the account shall not be reactivated based on the request of the account owner, unless the court issues a decision.

The National 24/7 Point of Contact of France has said that except for the orders of judicial authorities, the power to suspend bank accounts has not been granted to law enforcement officials. In addition, they have said that the suspension of an account is only limited to the amount of money related to the suspicious transaction and that the account owner may continue to use the

account. Banks may not conduct ex officio suspension of transactions with the exception of the situations specified in Articles 561 and 562 of the Financial Affairs Law of France (COMFI). In such exceptional cases, when the conditions, such as the financial crime unit of the requesting country contacting its French counterpart and such request being approved by the French Interbank Community, are met, the bank may suspend the account ex officio until a legal order is provided. Furthermore, banks may also follow this procedure among themselves due to the liabilities arising from international agreements. In case the banks do not fulfil their obligation to identify suspicious transactions, legal and criminal liabilities shall arise towards those who have suffered damages as per the law on LCBFT (Lutte Contre Blanchiment et Financement du Terrorisme). The client has the legal right to challenge the suspension of the account and if not found acting in bad faith, damages arising due to account suspension shall be compensated by the state. Lastly, since the money transferred to the account through a suspicious transaction may only be returned to the requesting country through a court decision, An MLA request must be initiated.

The National 24/7 Point of Contact of Latvia has indicated that, in the case of suspicious transactions, a bank account could be suspended for 45 days until a court decision is issued. If no action is taken by the end of this period, the account will be reactivated automatically. It has also been pointed out that within the scope of the Law on Seizure of Unlawfully Acquired Property, the victims may file for compensation of the damages that occur as a result of the bank's failure to suspend the account subject to suspicious transaction.

2.12 Question 12 – The power of LEA to suspend bank accounts

In some countries, law enforcement officers are able to suspend accounts ex officio in cases of money laundering, financing of terrorism and emergency situations.

- **Explain your opinion on the conditions and limitations of using such a power and in terms of its conformity with the Turkish legal system.**
- **What kind of regulation or practices can be developed for taking preventive measures in a timely manner by rapidly bypassing the legal procedures in order to fight effectively cybercrime?**

Most of the participants have said that law enforcement officials could be granted the power to suspend bank accounts ex officio in emergency situations. However, they have also added that administrative decisions reached based on such an authorisation must be submitted to

judicial authorities within 24 hours in compliance with the Turkish Penal Code and an effective judicial review must be sought.

Currently existing practices have also been addressed by the participants. Within the scope of Law no. 5549, banks report suspicious transactions to MASAK. Reports prepared on the bank accounts suspended for a maximum of seven days are submitted to the Public Prosecution Offices. As per Article 128 of the Turkish Criminal Procedure Code, the decision to seize accounts can be taken by the justice of the peace during the investigation stage, the court during the prosecution stage, and the Public Prosecutor when a delay is not desirable to be submitted later to a competent judge. The participants have also indicated that an administrative board formed under Law no. 6415 has also been equipped with similar authorities and has been left outside of the judicial review, in contrast to the current practices.

The 24/7 National Point of Contact of Latvia has stated that if the requesting country is a member of the Egmont group, requests related to laundering of criminal proceeds should be submitted to the Financial Crime Unit of Latvia or letters rogatory should be sent.

2.13 Question 13 – The requirement of having statements from foreign victims in cases of fraud

According to paragraph 1/f of Article 158 of the Turkish Penal Code, offenses of fraud committed by using data processing systems, banks and financial institutions as a tool, are considered as aggravated crime. In practice, especially in the beginning of the investigation statements from foreign victims are required and a criminal case is not initiated if the statements are not received. Discuss the reasons for this practice and its conformity with the Turkish legal system.

Most of the participants emphasised that following-up on offenses committed within the scope of Article 158 paragraph 1/f of the Turkish Penal Code is not subject to complaints and the investigation should be conducted ex officio without the statements of the victims. Some participants have pointed out that of taking a decision for non-prosecution of cases where the victim or the complainant is abroad is a bad practice.

One participant has presented an opposing view, indicating that the suspect must engage in a deceiving act and that the complainant must be deceived for the offense of fraud to occur. It is not possible to decide whether the element of deception plays a role without the statement of the

victim. Therefore, it has been indicated that the current practice is not contradictory to the Turkish legal system.

2.14 Question 14 – Use of data after retention period expires

According to law no. 5651, Internet Service Providers in Turkey must retain traffic data from 6 months to 2 years. Assume that the relevant letter rogatory reached our country a long time after the maximum duration of storage ended. But the Internet Service Provider has not deleted the data and our judicial authorities have sent the data to the relevant requesting country.

a. **The suspect asserts that data have lost the quality of evidence for the charges brought against him/her and therefore, claims in court that they must be considered as inadmissible. Examine this claim in the context of the Law on the Protection of Personal Data and the Criminal Procedure Code.**

b. **Later on, the suspect files a case against the Internet Service Provider on grounds that their personal data were stored unlawfully. According to the legal regulations in our country and the General Data Protection Regulation (GDPR) of the European Union, does the Internet Service Provider bear any legal liability?**

c. **This time, the Internet Service Provider automatically deletes the preserved data when the maximum duration of storage comes to an end. Right after the data being deleted, the letter rogatory is received. Could the requesting country accuse the Internet Service Provider on grounds that the personal information should be exempt from the obligation to protect since the concerned data are related to a criminal investigation? Is there any contradiction with the Law on the Protection of Personal Data?**

It has been indicated that since the data preservation request in option A is received from abroad, whether data obtained after the end of the legal storage period is accepted must be reviewed according to the laws of the relevant country.

One participant, referring to the German Penal Code, has drew attention that decisions in Germany are reached by balancing the right which is being violated and the right being protected, thus data which was not deleted in Turkey despite exceeding its maximum period of storage

would be accepted in Germany as evidence.

If option A is adopted to a suspect in Turkey; in other words, if data retained by another country for more than two years is reaching the court, the evidence would not be considered as lawfully obtained on the basis of Article 217 of the Criminal Procedure Code. One participant did not agree with this dominant view, claiming that evidence is in conformity with the law once they are retained. Based on the assumption that the data is not false, their status as evidence would be maintained even if the maximum period of retention expired.

Regarding the data retained for longer than the maximum period, most of the participants have also agreed that the service providers would be committing the offense of "failure to destroy data" defined in Article 138 of the Turkish Penal Code. But some participants have conveyed an opposite view by drawing attention to the difference between destroying data and erasing data as stipulated in Law no. 6698. According to the regulation adopted in accordance with the said law, data processors are unable to access the relevant data after they have been erased, while no one is able to access them after they have been destroyed. The participant has suggested that a period of 10 years could be identified for destroying data, as is the case in the Turkish Code of Obligations, and that the data erased at the end of 2 years could still be accessed by judicial authorities for 10 years. Since data will not be destroyed this way, service providers will not be held liable under Article 138 of the Turkish Penal Code and judicial authorities will have the opportunity to obtain digital evidence during investigation and prosecution that may last for many years.

Similar discussions have been held on the legal rights of the suspect concerning data not erased/destroyed at the end of two years, as put forth in option B. While most of the participants have claimed that the offense of "not destroying data" would be at stake, one participant has argued that preserving data for a longer period would be in compliance with the law, given that it is identified transparently in the company's policy and reasonable causes exist as in the abovementioned example.

Concerning option C, full consensus has been reached on the fact that the service provider would not be held legally liable since it has complied with the periods specified in Law no. 5651 and has erased the relevant data at the end of the 2-year period.

The National 24/7 Point of Contact of Latvia has noted that digital data are retained by service providers for a maximum period of 18 months and theoretically these data cannot be used as evidence against suspects after this period has expired. The Point of Contact has also stated that even if the maximum period for retention has been exceeded, the decision-making authority on whether the data would qualify as evidence is the judicial authority and if such a judicial decision is reached, the legal and criminal liability of the service provider would no longer exist. In case

data, considered unlawful, are kept and used after its maximum retention period has expired, suspects have the right to legally challenge; however, no such case has been observed in practice.

In addition to these, the National 24/7 Point of Contact of France has emphasised that the boundaries of the data sharing with other countries has been regulated by the GDPR and service providers may face severe sanctions in case of acting in contradiction with the GDPR.

2.15 Question 15 – Real-time collection and partial disclosure of traffic data

Articles 17 and 20 of the Convention allow preservation and real-time collection and partial disclosure of traffic data. Article 21 allows parties to obtain content data. Assume that an organised criminal group is communicating with each other on a forum of a website accessed only by its members about an illegal arms trade that is. The server of the website found in our country automatically deletes the conversations five minutes after the communication is ended. Country A needs traffic data in order to be able to identify the members of this crime group in their country.

- **In legal terms, is it possible to perform real-time collection of the traffic data in our country and to share the part of this information that will be helpful in identifying the suspect and victims abroad with the other contact points regarding immediate assistance?**
- **If your answer is yes, are they authorised to implement this security measure for types of offenses indicated in Article 135 of the Criminal Procedure Code or could its scope be kept more comprehensive?**
- **If your answer is no, what kind of legislation and implementation should be developed for this case?**

Different technical, organisational and legal views have been presented in terms of real-time collection of traffic data within the scope of Article 135 of the Criminal Procedure Code. Most of the participants have claimed that the measure of intercepting correspondence cannot be applied for the offenses other than the catalogue of offenses listed in Article 135. Mentioning that traffic data do not contain information about the content of communication, one participant has said that the measure of identifying the communication, defined in paragraph 5 of the relevant Article, could be applied. The measure of identifying communication, which is known in practice as HTS in Turkey and which includes the call detail record and the base stations through which

connection to the targeted phone numbers are made, may also be used for offenses other than those that are strictly listed in Article 135 of the Criminal Procedure Code.

Another participant has noted that in the abovementioned example, since data have been stored in the server for 5 minutes, the case cannot be considered as communication in real-time and a digital forensics examination must be conducted by seizing the relevant server within the scope of Article 134 of the Criminal Procedure Code.

It has been conveyed that in the current situation, real-time traffic data cannot even be shared partially with other National 24/7 Points of Contact without making a legislative amendment and the process of letters rogatory must be executed.

In terms of technique and organisation, the participants have identified as the greatest obstacles the lack of technical ability or the willingness of local and foreign content providers to cooperate in performing real-time collection of traffic data and the existing data and practices that have been dispersed in different countries due to the widely-used cloud computing solutions.

Regarding accessing data found in the cloud for a digital forensics' examination, one participant has said that authorisation has been granted to law enforcement officials for searching and backing up remote computer logs as per Article 17 of the Regulation on Forensic and Interception Examination. However, they have also added that this issue is controversial in legal terms and inconvenient in terms of national sovereignty since a similar authorisation is not defined in the Criminal Procedure Code.

The National 24/7 Points of Contact of Latvia and France have stated that it is possible to perform real-time collection of traffic data in their countries. While the domestic law of France permits this measure for investigations against terrorism and organised crimes, it does not consider traffic data requested on a regular basis from service providers as personal data.

2.16 Question 16 – Real-time interception of content data

Assume that another organised criminal group is forcing little children to sell their sexual images live online in return for money (Webcam Child Prostitution/Live Streaming Child Abuse on Demand) through VoIP (Voice-over-IP) technology. Different from traditional crimes, the video chat between the victim and suspect is the only factor constituting the criminal act and the evidence of the crime. Unless one of the parties records the conversation through different applications, it is not possible to find any other evidence

related to the criminal act. In this example, the victims and perpetrators are in different countries, but the VoIP service provider is found in our country. Since VoIP services are closely related with persons' rights and freedoms of communication, the Internet Service Provider only collects subscriber information automatically. In order to identify the victims and to reveal the only evidence of the live online child abuse, country A asks us to perform real-time collection of content data pertaining to a particular suspect and to share the data with them.

- **In the current situation, all countries have legitimate authority to intercept communication. According to the Turkish legal system, particularly including Articles 135 and 140 of the Criminal Procedure Code, is there sufficient legal basis for taking this measure in online platforms?**
- **In order to prevent physical child abuse that is likely to occur in country A, is it possible to rapidly share these data that have been collected through exceptional measures?**
- **Assume that a legal basis exists/is formed, and that the relevant judicial decision is presented to the relevant service provider. By pointing out that the VoIP system is based on the principles of an end-to-end encryption and P2P distributed network that makes the intervention of a third party, including themselves, impossible, the service provider indicates that abiding by the decision is virtually impossible. Please express your views on the practical and legislative regulations that could be implemented in such a case.**

The participants have stated that the collection of real-time content data could be performed theoretically according to Article 135 of the Criminal Procedure Code, but there are technical and practical conditions that make this sometimes impossible in practice. One participant has conveyed that since communication data is encrypted, procedures can also be performed within the scope of Article 134 of the Criminal Procedure Code. Another participant has explained in detail the necessary technical conditions for intercepting contents of popular VoIP (Voice-over-IP) applications abroad and social media platforms used in Turkey. In this respect, the conditions for transferring content and traffic data generated by the abovementioned applications to the servers in Turkey and obtaining the source codes of these software must be fulfilled together. Most participants have said that achieving this is highly unlikely and that it will not be able to create the desired effect even if it is carried out. The moderator has made a general reference to the encryption debate that has recently intensified and has given brief information on law enforcement officials gaining access to the applications in certain cases, keeping the special keys used in communication in an independent institution and establishing the responsibility to provide information for service providers through legislative regulations. However, most of

the participants have emphasised that hundreds of similar applications currently exist, and users shall quickly start looking for alternative applications and could even develop new technological solutions.

With regard to sharing real-time content data to identify the suspect and victim and to prevent the ongoing case of abuse, the participants have said that there is a lack of legislative regulation both in the Convention text and in domestic law. Therefore, it has been conveyed that it would be more appropriate to first issue a preservation request and then to share information when the letters rogatory is received. One participant has said that the Convention allows information to be shared in serious cases as in the aforementioned example and has underlined that if the necessary legislative regulations are made in domestic law, it could be possible to share intelligence related information to a certain extent as defined by the court decision. The same participant has also mentioned that the current legislation is not suitable for such quick interventions. Another participant has drawn attention to the fact that content of communication and its logs are subject to special procedures and if the content is shared, difficulties could be experienced especially in terms of the liability of destroying data.

2.17 Question 17 – Spontaneous information

Intelligence agencies obtain conversation records between two terrorist organisation members living in country A. Neighbours indicate that these two persons are planning an attack on an airport located in our country.

- **Article 26 of the Convention gives parties the right to forward information ex officio. Do you think that information collected by intelligence can also be considered and shared within this framework? Or, should this Article be considered exclusively within the scope of criminal investigations and proceedings?**
- **Assume that country A also obtained the same information from the intelligence agencies with the help of an informant. Country A contacts the Internet Service Provider and obtains the subscriber information of the two terrorists. However, country A does not provide any information to the National Point of Contact regarding the matter. Following a deadly attack, the National Point of Contact becomes aware of country A's negligence in this event through the Internet Service Provider. What kind of legal and diplomatic steps could be taken against country A?**

Most of the participants have noted that Article 26 of the Convention also allows sharing of intelligence-related information. Indicating that reciprocity and good will are the dominant principles of international law, one participant has emphasised that information could be shared for all kinds of criminal investigation or intelligence efforts within the limits drawn by these universal principles.

Some participants have stated that the term "investigation" mentioned in the Convention could exclude intelligence activities. The moderator has added that unlike in Turkey, collection activities of intelligence-related information are also considered within the concept of criminal investigation in many countries.

One participant who has provided an opposite view has said that the information to be shared, as stipulated in Article 26, should be obtained from a criminal investigation. They have added that this criminal investigation must relate to the cybercrimes defined between Articles 2 and 11 of the Convention and that within the scope of Article 26, it is not possible to share information with the other 24/7 Points of Contact for a terrorist attack as described in the abovementioned example.

The participants have conveyed different views on losses occurring as a result of critical information not being shared. Some of them have indicated that diplomatic channels could be used for foreign points of contact, while general provisions like "neglect of duty", as stated in the Turkish Penal Code, could apply for the 24/7 Point of Contact. Another participant, who remarked that this Article does not impose any obligation on the National Point of Contact and gives them discretionary power on sharing of information, has claimed that no criminal liability of any kind shall arise.

Pointing out that the laws of Latvia authorises sharing of intelligence-related information; the National 24/7 Point of Contact of Latvia has marked the limits of this measure for service providers and the National Point of Contact. In cases where delays are considered as a drawback and which could cause irrecoverable or irreparable damages, the service provider and the National 24/7 Point of Contact may transfer information to the extent that these damages would be prevented. In the event of providing more information than needed or other cases of abuse, legal and criminal liability shall arise for the protection of personal data. The 24/7 Point of Contact of France has drawn attention to the literal provision of the Convention, stating that sharing of intelligence-related information is not an obligation and that there are alternative communication channels like Interpol.

2.18 Question 18 – Sharing information through e-mails and direct co-operation with ISPs

Within the framework of bilateral and multilateral agreements, Turkey conducts police cooperation activities together with other countries and with international police organisations like Interpol. However, the Budapest Convention is an exceptional text that foresees faster decision-making and information sharing than traditional methods, primarily with the objectives of urgently preserving digital data and rapidly identifying the victims and suspects. Express your views on the below mentioned matters in terms of legal and organisational solutions for an effective international police cooperation to be implemented and information/data to be shared in the fastest way possible as foreseen in the Convention.

- **National Points of Contact in some countries have fast communication channels with all the local service providers in the country, mostly through e-mail. Is it possible in legal and administrative terms for such a system to be established in our country? If not, what kind of changes should be made in this respect?**
- **The National Point of Contact can obtain information directly from various foreign Internet Service Providers. Moreover, a draft law is currently being discussed that enables police organisations, which are members of the European Union, to be able to directly request information from Internet Service Providers found in other countries. Within this framework, indicate the suitability, conditions and limits of a foreign security unit being able to directly request information from an Internet Service Provider based in Turkey.**

The moderator has started the discussion by indicating that certain Internet Service Providers based in the US are able to directly provide subscriber information to foreign law enforcement officers and that the communication between the US-based Internet Service Providers and the National 24/7 Point of Contact of the US mostly takes place through e-mail.

All of the participants have conveyed their concerns on the performance of direct information flow from service providers based in Turkey to the foreign National 24/7 Point of Contact. Claiming that Internet Service Providers based in the US form such direct communication channels because they aim to gain commercial profit, a participant has put forward the idea that service providers based in Turkey would not need such a practice since they do not have a customer base of a similar size to the US or other countries.

The majority of participants have said that when sharing information internationally, reciprocity, the foreign policy of the country and conformity with domestic law should be considered critical and have indicated that eliminating all judicial and diplomatic channels would create undesirable consequences. One participant has said that US-based Internet service providers probably inform the authorities in the country on a frequent basis and that the external inspection mechanism for the direct sharing of information should also be regulated if a similar implementation is brought into effect in Turkey. By indicating that such authorisation is directly related to the sovereignty rights of states, another participant has said that a one-sided legislative regulation made in domestic law would not be sufficient unless member states grant each other mutual authorisation based on an international convention.

All participants have agreed that faster communication should be established in the country through e-mail between the National 24/7 Point of Contact and the service providers based in Turkey. Some participants have emphasised that service providers deal with sensitive personal data and that it is obligatory for a regulation to be adopted concerning the content of the data to be shared with the National 24/7 Point of Contact. One participant has stated that transferring information through e-mail, particularly for the expedited execution of the preservation requests, has become an obligation and is no longer an option. In technical terms, the prevailing view has been that information should be shared using e-mail addresses defined beforehand through reliable systems, such as the Registered E-mail Service (KEP) or the National Judicial Network System (UYAP), in order to maximise the security of communication between the two parties.

3 Conclusion

Various views of participants coming from different backgrounds of specialisation have been conveyed during the workshop. Certain issues have been emphasised repeatedly throughout the event by many participants. Namely, the necessity for comprehensively transposing the Convention in letter and spirit into domestic law has been highlighted by most of the participants. While the Convention makes a distinction between subscriber information, traffic data and content data, subscriber information within the Turkish law is defined as an extension of the traffic data, while content data is not defined yet. Similarly, the Law no. 5651 on "Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication" makes a four-way distinction between access, hosting, content and public use providers in terms of legal responsibilities; the Convention only uses the term service provider. These differences in definitions provided in the Convention and domestic law, discussed particularly on the first day of the workshop, have caused confusion of concepts and misinterpretation.

Another issue expressed frequently during the workshop is the need to clarify the scope of duties and powers of the National 24/7 Point of Contact and the Internet Service Providers through regulation. Most of the participants have not considered it sufficient to rely exclusively on the Convention for data preservation requests and international sharing of information in emergency situation. Reinforcing the legal framework through new regulations has been pointed out as an absolute prerequisite for ensuring compliance with the Convention in Turkey.

4 List of participants

Moderator

Kemal Veli AÇAR	Unit Manager	Turkish National Police Department of Cyber Crime

Participants

Erdal ÇETİNKAYA	Head of Department	Turkish National Police Department of Cybercrime
Kerim ALTIAY	Deputy Head of Department	Turkish National Police Department of Cybercrime
İbrahim ÖZDEMİR	Inspector	Turkish National Police Department of Cybercrime
Murat Volkan DÜLGER	Associate Professor Doctor	Istanbul Aydın University
Hasan SINAR	Associate Professor Doctor	Altınbaş University
Yavuz ERDOĞAN	Associate Professor Doctor	European University of Lefke
Özgür KARLITEPE	Unit Manager	Turkish National Police Istanbul Cybercrime Unit
Mehmet PAKİŞ	Judge	The Court of Cassation
Ömrü YILMAZ	Judge	The Court of Cassation
Ayla SERÇE	Asistant Expert	Ministry of Justice Directorate General for International Law and Foreign Relations
Mehmet YILDIZ	Superintendent	Turkish National Police-Interpol-Europol Department
Mahmut Kaan YÜKSEL	Prosecutor	Ankara Prosecutor's Office
Murat SEMİZ	Prosecutor	Istanbul Prosecutor's Office
Baki Çağrı ONGUN	Judge	Istanbul Courthouse
Soner KAYA	Prosecutor	Izmir Prosecutor's Office
Enes Koray KOÇAK	Inspector	Turkish National Police Department of Cybercrime
Kadir BAĞCI	Judge	Ministry of Justice General Directorate of Criminal Affairs
Ceren KÜPELİ	Lawyer	Turkcell Communication Services Inc.

Burhanettin AL	Lawyer	Turkcell Communication Services Inc.
Ayşe ŞEKER	Manager of IT Law	Türk Telekom Inc.
Çağrı YALÇIN	Lawyer	Türk Telekom Inc.
Osman Özkan NAZLIM	Police Officer	Turkish National Police Department of Cybercrime
Mustafa SAĞLAM	Police Officer	Turkish National Police Department of Cybercrime
Gökhan BOZDOĞAN	Director of Technology Security Operations	Vodafone Inc.
Sait REÇBER	Privacy Director	Vodafone Inc.
Emre ERGİN	Lawyer	Vodafone Inc.
Yeliz KILIÇ	Lawyer	Ministry of Interior - Office of Legal Counsellor
Muhammed DÜLGERLER	Lawyer	İsimtescil Inc.
Engin PURCU	Police Officer	Turkish National Police Istanbul Cybercrime Unit
Müşerref ÇUHADAR	Deputy Inspector	Turkish National Police-Department of Foreign Relations
Ali Rıza ÇELİK	Superintendent	Turkish National Police-Department of Foreign Relations
Mehmet UÇAR	IT Manager	İsimtescil Inc.
Özgür ÖZCAN	System Manager	Mynet.com Inc.

Two Experts from the Information Technologies and Communication Authority*

One Expert from the Turkcell Communication Services Inc.*

One Judge from the Ministry of Justice*

Foreign Guests

France, 24/7 National Point of Contact*

Latvia, 24/7 National Point of Contact*

Romania, 24/7 National Point of Contact*

* The participant requested to stay anonymous

İncek Mahallesi Boztepe Sk. 06830 Gölbaşı / Ankara
Turkey
+90 312 462 55 00
+90 312 286 92 06
siber@egm.gov.tr