FIGHTING CRIME IN THE KNOWLEDGE SOCIETY: REFLEXION ABOUT TURKISH CRIMINAL CODE

Pinar MEMIŞ KARTAL*

Abstract

The state has the negative and positive obligation to not violate basic rights of human rights. But the state also must fighting crime. As in legal systems of many countries, evidence and substantiation of cybercrime under Turkish law constitutes an issue of major importance. Inadequacy of legislation, discrepancies between national law and initiatives in international judicial cooperation, lack of specialized authorities, shortage of personnel and experts with knowledge and expertise in cybercrime, and absence of specialized prosecutors and courts on cybercrime are factors which contribute to difficulties in fighting cybercrime.

Keywords: *knowledge, society, penal law, penal prosecution, proof, evidence, forensic cybernetics.*

1. Introduction

The state has the negative obligation to not violate basic rights of individuals through its interactions. The state also has a positive obligation to protect human beings from basic rights' violations.[1]

The most important discoveries of modern times, information technology and the internet have become indispensable in enhancing our lives, but it has also become a tool for illegal activities in parallel with developing technology and human nature, thus making it one of the more important topics of penal law. It stands out as a topic which creates unique challenges for penal law due to its cross border structure, intangible medium and the fact that perpetrators cannot be identified easily, even if the illegal act itself is. This is a challenge not only for lawyers but for everyone involved in information technology. Although there are various legislative and regulatory acts in Turkish law on the subject, these tend to remain inadequate due to its tight link to technological developments and its complexity[2].

Cybercrime can be broadly categorized into two main subtopics which are crimes against information systems and crimes committed through the internet.[3]

* Associated Professor, Ph.D., Faculty of Law, „Galatasaray" University, Istanbul (e-mail: pinarmem@gmail.com). The study has been orally presented by Mrs Pinar MEMIŞ-KARTAL in her quality of keynote speaker of the 11th edition of the International Conference *Challenges of the Knowledge Society* (CKS), held in Bucharest (Romania), on May 12th, 2017 (please see the CKS 2017 program available at http://cks.univnt.ro/cks_2017.html).

[1] *Yenisey Feridun*, (2020) "Crimes Against Pollution Caused by Illegal Construction in Turkey," Journal of Comparative Urban Law and Policy: Vol. 4 : Iss. 1 , Article 21, (311-323), 311.

[2] *Kunter Nurullah*/ *Yenisey Feridun* / *Nuhoğlu Ayşe*, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Beta, Ekim 2010, p.1093; *Centel Nur/Zafer Hamide*, Ceza Muhakemesi Hukuku, Beta, Ekim 2011, p.400; *Bıçak Vahit,* Suç Muhakemesi Hukuku, Seçkin, Ankara 2010, 581.

[3] *Gedik Doğan*, "Bilişim Suçlarında IP Tespiti İle Ekran Görüntüleri Çıktılarının İspat Değeri", in: Bilişim Hukuku Dergisi, 2019, (51-84), 53.

When legal values protected by these crimes are taken into account, it is readily apparent that they are closely connected to fundamental rights and freedoms. In particular, personal security, right to privacy and freedom of expression are fundamental rights and freedoms protected by multinational conventions (ECHR) and constitutions (Art. 17, 19 and 20 of the Turkish Constitution), which can become manifest in or through information technology. The fight against cybercrime also has an international dimension. The "Convention on Cybercrime" which was opened to accession on November 23rd, 2001 has been ratified by many countries. Turkey has finally acceded to this convention on November 10th, 2010. However the treaty has yet to be ratified by the Turkish Parliament in order to become enforceable nationally. The treaty prescribes new investigative methods in the fight against cybercrime. Kunter/Yenisey/Nuhoğlu agreeably contend that the treaty should be ratified and that under Article 13 of the Constitution of the Turkish Republic, such methods have to be prescribed by parliamentary acts, since they encroach upon rights and freedoms of individuals, in particular the right to privacy[4].

Criminal offences such as unauthorized access to, interference with or damaging or destroying information systems can also be used to commit offences such as insulting, violation of the confidentiality of communications, violation of privacy, recording and assembly of personal data for illegal use, praising criminal offences and discrimination, through the internet. Such acts are offences in and of themselves, whereas commission of such crimes through the internet will constitute an aggravating factor for some of them.

With the above framework in mind, in this article I will try to provide some general advice on current legislation concerning matters of evidence and proof, the general approach of penal procedure to the subject, and methods which can be employed to attain substantive truth in cybercrime. Although this framework also involves forensic cybernetics as a sub-discipline of forensic science, I will not delve into technical details as it is beyond the scope of my area of expertise[5].

2. Fighting Crime with the Turkish Criminal Legislation

The intangible and virtual nature of information technology makes the search for truth a very difficult task, and renders the proof of cybercrime problematic. The problem of proof in cybercrime thus constitutes a major topic in penal law and procedure in view of the aforementioned nature of information technology.

2.1. Crimes against knowledge society: Examples in the Turkish Criminal Code

It is readily apparent that there are loopholes in Turkish penal legislation on cybercrime which is broadly categorized into two main areas\ which are offences against information systems, and offences committed through the internet.

The criminal offences of "unauthorized access to an information system" (TCC Art. 243), "blocking an

[4] K*unter/Yenisey/Nuhoğlu*, (Fn 2), 1094.

[5] For more information about this famework also involves forensic cybernetics as a sub-discipline of forensic science., *Henkoğlu*; Adli Bilişim-Dijital Delillerin Elde Edilmesi ve Analizi, Pusula, Eylül 2011; *Karagülmez*, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin, Ankara 2011; K*unter/Yenisey/Nuhoğlu*, (Fn 2) 1106-1108.

information system" (TCC Art. 244) and, "abuse of bank and credit cards" (TCC Art. 245), the latter being somewhat disputed as to whether it is cybercrime although there is obviously a connection, have been regulated in the subsection 10 titled "Crimes in Cybernetics" under section 3 titled "Crimes Against Society" in the second main section of the Turkish Penal Code which defines specific crimes. It is not the purpose of this article to examine these crimes therefore suffice it to say that these are "cybercrimes" in which the lawful interest to be protected is the data contained within information systems[6].

Another piece of legislation on cybercrime is the Law No. 5651 on "Regulation of Publishing on the Internet and Prevention of Crime Committed Through These Publications"[7]. The law regulates responsibilities of service, content and access providers, situations where access can be prohibited judicially (such as incenting to suicide, sexual abuse of minors, facilitating use of narcotics, obscenity, prostitution etc.), right to respond, but no new cybercrimes have been defined. This Law No. 5651 consists of 14 articles and is clearly inadequate. Within the Turkish Criminal Code (Law. 5237), libel, violation of privacy, obscenity, sexual abuse of minors and various other crimes mentioned here above have been defined as criminal acts. Commission of these crimes on or through the internet do not constitute a separate offence, but in most cases it is an aggravating factor.[8] It may not be imperative to define new types of offences separately within legislation on prevention of crime on the internet, but there is a need for separate appropriate regulation of internet crimes. By appropriate regulation, what is meant is special methods and procedures for investigation and prosecution under the main subject of cybercrime. Creating a new definition of crimes besides the already existing provisions of the Turkish Criminal Code can lead to confusion and conflicts between provisions, making an already difficult situation even worse. The preferred approach will be to revise and update, and to develop investigation and prosecution methods appropriate to the offences defined, and to promulgate legislation which will enable discovery of evidence without violating essential fundamental rights and freedoms.

2.2. Fighting crime with the Turkish Code of Penal Procedure

Investigation and prosecution of cybercrime is undertaken according to the generally applicable rules of criminal procedure. This means that there are no provisions regarding collection and interpretation of evidence and proof which are specific to cybercrime.

Investigation and prosecution of cybercrime, or more specifically crimes against information systems and crimes committed through the internet, is quite distinct and different as compared to other crimes. The importance of the issue with regard to criminal procedure, the objective of which is to seek and uncover the substantive truth, is self evident in view of the nature and speed of information systems which require special techniques and expertise. Aside from problems likely to be encountered in investigating, identifying , collating and preserving evidence,

[6] *Tezcan Durmuş/Erdem Mustafa Ruhan/ Önok Murat,* Teorik ve Pratik Ceza Özel Hukuku, Seçkin, Ankara 2019, 1145-1148.

[7] The Law No. 5651 on "Regulation of Publishing on the Internet and Prevention of Crime Committed Through These Publications" entry in to force on 23.05.2007 at Official Gazette no:26530.

[8] *Dülger Murat Volkan*, Bilişim Suçları ve İnternet İletişim Hukuku, 2. Baskı, Seçkin, Ankara, 665 ets.

admissibility of the evidence can become an issue as such activities are inevitably linked to privacy rights, personal data and integrity of communication. Dealing with evidence closely related to fundamental rights and freedoms is a prominent feature of investigation of cybercrime.[9] Investigation of cybercrime where there is a high likelihood of breach of fundamental rights and freedoms require and deserve to be regulated separately and in specific detail.

Currently, collection of evidence in cybercrime is conducted in accordance with the provisions of the general legislative instrument in this area, which is the Code of Penal Procedure, Law no. 5271[10]. The problem which needs to be addressed in this regard is not only collection of evidence, but also the manner and duration of its preservation.

2.2.1. Investigation Phase

In investigating cybercrime, public prosecutors and the police use Art. 134 of the Code of Penal Procedure. This article regulates "Search, Copying and Confiscation of Computers, Computer Programmes and Registers". Although the title of this article suggests a provision specific to cybercrime, this is actually not the case as it is applicable to the investigation of any crime. Unver/Hakeri rightfully contend that lack of regulation on "*search on internet registers with or without data transfer*" is a shortcoming[11].

Kunter/Yenisey/Nuhoğlu argue that a distinction must be made in the admission of data found on the internet or an information system, as evidence in penal procedure[12]. The most recent date of recording must be taken as the basis for data stored on an information system. Another principle concerns data transferred to other locations. This requires scrutiny of such data by public authorities based on residual data transfer signals (CPP Art. 135) which requires a mandate different from that stipulated in CPP Art. 134. Writers on matters of evidence in information systems correctly point out that a court needs to issue two separate injunctions on these two separate issues. One of these is search on computer registers regulated in CPP Art. 134 and the other is monitoring of communications as regulated by CPP Art. 135[13]. Elimination of this ambiguity and facilitating timely and lawful access to evidence requires a new type of precautionary injunction appropriate to the nature of cybercrime.[14] Kunter/Yenisey/Nuhoğlu[15]. have pointed out that a new type of warrant should be created for access to encrypted data, with reference to the Treaty of the European Council dated 23.11.2011 and as set out by the norms of the European Parliament (2001/2070 COS, OJ C72E.21.03.2002,pp.323-329).

There also exists a "Regulation on Judicial and Preventive Searches", promulgated under the Code of Penal Procedure. Art. 17 of this regulation is a provision similar to that in the Code itself, in more intricate detail.

Both of these legislative texts are important to our subject matter, although it must be emphasized that they are not tailored or specific to cybercrime.

[9] *Gedik*, Bilişim Suçlarında IP Tespiti, 54.
[10] *Ünver Yener/Hakeri Hakan*, Ceza Muhakemesi Hukuku, 4. Bası, Adalet, Mart 2011, 424-427.
[11] *Ünver/Hakeri*, (Fn.6), 426.
[12] K*unter/Yenisey/Nuhoğlu*, (Fn 2), 1097.
[13] K*unter/Yenisey/Nuhoğlu*, (Fn 2), 1097-1098.
[14] *Kara İlker,* Dijital Kanıtlarının İncelemeleri ve Hukuki Boyutu, Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü, C.24, S.3, 2019, 184.
[15] K*unter/Yenisey/Nuhoğlu*, (Fn 2), 1098.

2.2.2. Prosecution Phase

Prosecution means the phase where an indictment by the prosecutor is accepted by the criminal court thereby commencing the criminal trial. The activity of collecting evidence is continued in this phase, subject again to the Code of Penal Procedure. However Art. 134 regulating the investigation phase will not be applicable in the prosecution phase. This Article explicitly provides that the rule is applicable only in the investigation phase.

Within this framework, inadequacies already inherent in the investigation phase are exacerbated in the prosecution phase. CPP Art. 116 which regulates search and confiscation in the pursuit for substantive truth is readily applicable in this phase. The Cybercrime Department of the Security Administration is charged with obtaining and evaluating evidence in the investigation of cybercrime. Technical proficiency and competence of department staff alone is far from being sufficient in itself in the struggle against cybercrime. Another department evaluating evidence obtained is the Physics Specialty department of the Institute of Forensic Sciences. Cybercrime is investigated also by this department, with mixed and disputed verdicts on the accuracy and authenticity of their findings[16].

3. Conclusion

Just like in many other countries, the problem of proof and evidence in cybercrime presents a major challenge in Turkish Law. Inadequacy of legislation, incompetence of national legislation with international cooperation, lack of specialized investigative authorities, shortage of staff proficient in cybernetics, lack of specialized prosecutors and courts are all important impediments in the endeavour for preventing cybercrime. Integrity and originality of data obtained from computers and the internet should be verified beyond doubt in order to be admitted as evidence, since such data can be manipulated and fabricated with impunity and very easily. [17].

As a first step, Turkish penal legislation needs to be reviewed from the point of view of cybercrime and methods and tools of collecting and evaluating evidence in this area should be regulated. More qualified security staff is needed in the struggle against cybercrime. Coordination and cooperation with international organizations in this area needs to be strengthened, and current developments need to be followed closely.

A separate independent Forensic Cybernetics Institute needs to be established, although this can also be within the structure of the existing Institute of Forensic Sciences, in order to properly preserve and evaluate evidence collected in the course of investigation and prosecution of cybercrime. It is not possible to expect prosecutors and judges to possess intricate technical knowledge on cybercrime. There are expert witnesses to cover this gap and an Institute of Forensic Cybernetics will be an important tool in evaluating evidence in cybercrime.

Judges and prosecutors as well need to gain a basic level of understanding in technical matters concerning cybercrime against information systems and crimes committed through the internet, although of course they cannot and should not be expected to have the level of knowledge that an expert on the subject can possess. It can be observed that in some European countries, some experts in cybercrime can

[16] *Öztürk Cemal*; İz İncelemede Adli Tıp Fizik İhtisas Dairesinin Yetki Sorunu, in, CHD-Ceza Hukuku Dergisi, Nisan 2001, Yıl:2, Sayı:1, Seçkin, 164-165.

[17] K*unter/Yenisey/Nuhoğlu*, (Fn 2), 1108.

possess degrees both in computer science and the law. Although it does not seem to be possible in Turkey at this time, this should be a very effective in preventing cybercrime.

References

- *Centel Nur/Zafer Hamide,* Ceza Muhakemesi Hukuku, Beta, Ekim 2011, p.400; *Bıçak Vahit,* Suç Muhakemesi Hukuku, Seçkin, Ankara 2010;
- *Dülger Murat Volkan*, Bilişim Suçları ve İnternet İletişim Hukuku (Cybercrime and Internet Communication Law), 2. Baskı, Seçkin, Ankara;
- *Gedik Doğan*, "Bilişim Suçlarında IP Tespiti İle Ekran Görüntüleri Çıktılarının İspat Değeri" ("Value as Evidence of Screenshots Obtained by IP Determination in Cybercrime"), in: Bilişim Hukuku Dergisi, 2019;
- *Henkoğlu*; Adli Bilişim-Dijital Delillerin Elde Edilmesi ve Analizi, Pusula, Eylül 2011;
- *Kara İlker,* Dijital Kanıtlarının İncelemeleri ve Hukuki Boyutu (Evaluation of Digital Evidence and its Legal Implications), Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü, C.24, S.3, 2019;
- *Karagülmez*, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri (Stages of Investigation and Prosecution of Cybercrime), Seçkin, Ankara 2011;
- *Kunter Nurullah*/ *Yenisey Feridun* / *Nuhoğlu Ayşe*, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku (Law of Penal Procedure as a Branch of Law of Procedure), Beta, Ekim 2010;
- *Öztürk Cemal*; İz İncelemede Adli Tıp Fizik İhtisas Dairesinin Yetki Sorunu (The Problem of Jurisdiction of the Forensic Institute Physics Department in Trace Evidence), in CHD-Ceza Hukuku Dergisi, Nisan 2001, Yıl:2, Sayı:1, Seçkin;
- *Tezcan Durmuş/Erdem Mustafa Ruhan/ Önok Murat,* Teorik ve Pratik Ceza Özel Hukuku (Penal Law Special Provisions in Theory and Practice), Seçkin, Ankara 2019;
- *Ünver Yener/Hakeri Hakan*, Ceza Muhakemesi Hukuku (Law of Penal Procedure), 4. Bası, Adalet, Mart 2011;
- *Yenisey Feridun*, (2020) "Crimes Against Pollution Caused by Illegal Construction in Turkey," Journal of Comparative Urban Law and Policy: Vol. 4 : Iss. 1, Article 21, (311-323).