KEYNOTE SPEECH BY PROF. DR. VAHİT BIÇAK TO BE ADDRESSED IN THE 6’TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSIC AND SECURITY (ISDFS 2018)

Turkish Law on Illegally Accessing or Preventing the Functioning of a Data Processing System or Deletion, Alteration or Corrupting of Data

Prof. Dr. Vahit Bıçak
Başkent Üniversitesi Hukuk Fakültesi
www.vahitbicak.com.tr

1. Introduction

Cybercrime remains a real and significant phenomenon, posing threat to not only the national security of Turkey, but also the public order of the whole world.[1] Ever-increasingly sophisticated criminal techniques and methods which have traditionally been associated with cybercrime are extending into other crime and threat areas. In other words, the boundaries between tradition crimes and cybercrimes blur. A growing range of threats, from trafficking in human beings to terrorism, are becoming increasingly cyber-enabled. The additional increase in volume, scope and financial damage combined with the asymmetric risk that characterizes cybercrime has reached such a level that in some countries cybercrime may have surpassed traditional crime in terms of reporting.[2]

One of the biggest challenges of combatting cybercrimes for law enforcement authorities is attribution. The growing misuse of legitimate anonymity and encryption services and tools for illegal purposes makes it hard for the law enforcement to detect the exact perpetrators, posing a serious impediment to investigation and prosecution of them, and creating a high level of threat cutting across all crime areas.[3] While it is of utmost importance to conduct e-commerce and other cyberspace activity in a safe and strongly encrypted manner, adoption of the same level of encryption by cyber criminals creates a serious impediment to effective and conclusive investigation of cybercrimes by police forces.

In an environment where even states reflect their animosity toward one another via resorting to cyber attacks – such as North Korea carrying out a cyber-attack on Sony in the

[1] Internet Organised Crime Threat Assessment (IOCTA), European Police Office (EUROPOL), 2016, s.7.

[2] Office for National Statistics, Crime in England and Wales: year ending Mar 2016, https://www.gov.uk/government/statistics/crime-in-england-and-wales-year-ending-mar-2016, 2016

[3] Internet Organised Crime Threat Assessment (IOCTA), s. 8.

US,[4] China's Mirai hackers knocking offline a whole group of major websites, including Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times by a massive DDoS attack,[5] Russia meddling in the 2016 US election through cyber means – perpetrators of traditional crimes develop new and sophisticated methods of committing crimes to keep up with their competitors and with law enforcement possessing better equipment and higher budgets allocated for combatting crimes. In that regard, cold war mentality ensues in the fight between criminals and law enforcement in the sense that each side of the war strives to acquire new technics and weapons due to the fear that the other side has already been equipped with the better ones.[6]

What distinguishes mafia from state is that the latter complies with what the law requires. With that in mind, law enforcement must conduct its fight against cyber criminals within the confines of law despite the criminals having no regard for rules and order. Therefore, legal aspect of this matter is of utmost significance in that the relevant laws draw up the way the law enforcement must proceed through. On the other hand, a set of rules specifically tailored for the needs and circumstances of the time would help the law enforcement to exercise its detection, investigation and prosecution in an efficient and result-oriented manner. Otherwise, the law would fail to keep up with technical and technological developments of the time, thus depriving the law enforcement of pertinent legal mechanisms whereby they conduct their fight in the cyber domain.

2. The Computer-related Offences under the Turkish Penal Code

That said, it is worthwhile to note that the Turkish legislation aiming at combatting cybercrimes have been enacted in line with the 2001 Budapest Convention on Cyber Crime, the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.[7]

The offences as to computer-related crimes envisaged in the Turkish Penal Code (TPC) are as follows:

> **Access to data processing system**
>
> **ARTICLE 243-**(1) Any person who unlawfully enters a part or whole of data processing system or remains there is punished with imprisonment up to one year, or imposed punitive fine.

[4] Lori Grisham, "North Korea and the Sony Pictures hack", *USA Today*, 18.12.2014.
[5] Brian Solomon, "Hacked Cameras Were Behind Friday's Massive Web Outage", *Forbes*, 21.10.2016.
[6] Osgood, Charles E. "An analysis of the cold war mentality." Journal of Social Issues 17.3 (1961): 12-19.
[7] Convention on Cybercrime, ETS No.185, Budapest, 23/11/2001
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

(2) In case the offenses defined in above subsection involve systems which are benefited against charge, the punishment to be imposed is increased up to one half.

(3) If such act results with deletion or alteration of data within the content of the system, the person responsible from such failure is sentenced to imprisonment from six months up to two years.

(4) Any person who unlawfully monitors the data transfers within a data processing system or between data processing systems through technical devices without entering the system is sentenced to imprisonment from one year to three years.

Hindrance or destruction of the system, deletion or alteration of data

ARTICLE 244-(1) Any person who hinders or destroys operation of a data processing system is punished with imprisonment from one year to five years.

(2) Any person who garbles, deletes, changes or prevents access to data, or installs data in the system or sends the available data to other places is punished with imprisonment from six months to three years.

(3) The punishment to be imposed is increased by one half in case of commission of these offenses on the data processing systems belonging to a bank or credit institution, or public institutions or corporations.

(4) Where the execution of above mentioned acts does not constitute any other offense apart from unjust benefit secured by a person for himself or in favor of third parties, the offender is sentenced to imprisonment from two years to six years, and also imposed punitive fine up to five thousand days.

Improper use of bank or credit cards

ARTICLE 245- (1) Any person who acquires or holds bank or credit cards of another person(s) whatever the reason is, or uses these cards without consent of the card holder or the receiver of the card, or secures benefit for himself or third parties by allowing use of the same by others, is punished with imprisonment from three years to six years, and also imposed punitive fine.

(2) Any person who secures benefit for himself or third parties by using a counterfeit bank or credit card is punished with imprisonment from four years to seven years if the act executed does not constitute any offense other than forgery.

Prohibited devices and programs

Article 245/A - (1) Any person who produces, imports, procures for use, transfers, stores, sells, distributes, purchases or otherwise makes available of a device, computer program, computer password, or similar access code, designed or adapted primarily for the purpose of committing any of the offences in this Section is punished with imprisonment from one year to three years, and also imposed punitive fine.

Imposition of Security Precautions on Legal Entities

> **ARTICLE 246-** (1) Security precautions specific to legal entities are imposed in case of commission of the offenses listed in this section within the frame of activities of legal entities.

There are some restrictions imposed on the law enforcement in terms of the procedures according to which they gather evidence. At the outset, it is worthwhile to stress that the Constitutional Court ruled (in its decision No. 2013/7800) "*digital data cannot be claimed to show the absolute reality*". Secondly, articles 134 and 135 of the Turkish Criminal Procedure Code (TCPC) set forth the procedures through which digital evidence can be obtained. Envisaging the procedure under which the law enforcement is allowed to seize and search electronic devices, Article 134 of the TCPC reads as follows:

> **Search of computers, computer programs and transcripts, copying and provisional seizure**
> **Article 134 –** (1) Upon the motion of the public prosecutor during an investigation with respect to a crime, the judge shall issue a decision on the computer programs and records used by the suspect, the copying, analyzing, and textualization of those records, if it is not possible
> to obtain the evidence by other means.
> (2) If computers, computer programs and computer records are inaccessible, as the passwords are not known, or if the hidden information is unreachable, then the computer and equipment that are deemed necessary may be provisionally seized in order to retrieve and to make the necessary copies. Seized devices shall be returned without delay in cases where the password has been solved and the necessary copies are produced.
> (3) While enforcing the seizure of computers or computer records, all data included in the system shall be copied.
> (4) In cases where the suspect or his representative makes a request, a copy of this copied data shall be produced and given to him or to his representative and this exchange shall be recorded and signed.
> (5) It is also permissible to produce a copy of the entire data or some of the data included in the system, without seizing the computer or the computer records. Copied data shall be printed on paper and this situation shall be recorded and signed by the related persons.

Article 135 of the TCPC also lays down similar restrictive procedures for interception of the correspondence via telecommunication:

> **Location, listening and recording of correspondence**
> **Article 135 –** (1) The judge or, in cases of peril in delay, the public prosecutor, may decide to locate, listen to or record the correspondence through telecommunication or to evaluate the information about the signals of the suspect or the accused, if during an investigation or prosecution conducted in relation to a crime there are strong grounds of suspicion indicating that the crime has been committed and there is no other possibility to obtain evidence. The public prosecutor shall submit his decision immediately to the judge for his approval and the judge shall make a decision within 24 hours. In cases where the duration expires or the judge decides the opposite way, the measure shall be lifted by the public prosecutor immediately.

(2) The correspondence of the suspect or the accused with individuals who enjoy the privilege of refraining from testimony as a witness shall not be recorded. In cases where this circumstance has been revealed after the recording has been conducted, the conducted recordings shall be destroyed immediately.
(3) The decision that shall be rendered according to the provisions of subparagraph 1 shall include the nature of the charged crime, the identity of the individual, upon whom the measure is going to be applied, the nature of the tool of communication, the number of the telephone, or the code that makes it possible to identify the connection of the communication, the nature of the measure, its extent and its duration. The decision of the measure may be given for maximum duration of 3 months; this duration may be extended one more time. However, for crimes committed within the activities of a crime organization, the judge may decide to extend the duration several times, each time for no longer than one month, if deemed necessary.
(4) The location of the mobile phone may be established upon the decision of the judge, or in cases of peril in delay, by the decision of the public prosecutor, in order to be able to
apprehend the suspect or the accused. The decision related to this matter shall include the
number of the mobile phone and the duration of the interaction of locating (the establishment). The interaction of locating shall be conducted for maximum of three months; this duration may be extended one more time.
(5) Decisions rendered and interactions conducted according to the provisions of this article shall be kept confidential while the measure is pending.
(6) The provisions contained in this article related to listening, recording and evaluating the information about the signals shall only be applicable for the crimes as listed below:
a) The following crimes in the Turkish Criminal Code;
1. Smuggling with migrants and human trafficking (Arts. 79, 80),
2. Killing with intent (Arts. 81, 82, 83),
3. Torture (Arts. 94, 95),
4. Sexual assault (Art. 102, except for subsection 1),
5. Sexual abuse of children (Art. 103),
6. Producing and trading with narcotic or stimulating substances (Art. 188),
7. Forgery in money (Art. 197),
8. Forming an organization in order to commit crimes (Art. 220, except for subsections 2, 7 and 8),
9. Prostitution (Art. 227, subparagraph 3),
10. Cheating in bidding (Art. 235),
11. Bribery (Art. 252),
12. Laundering of assets eminating from crime (Art. 282),
13. Armed criminal organization (Art. 314) or supplying such organizations with weapons (Art. 315),
14. Crimes against the secrets of the state and spying (Arts. 328, 329, 330, 331, 333, 334, 335, 336, 337).
b) Smuggling with guns, as defined in Act on Guns and Knifes and other Tools (Art. 12),
c) The crime of embezzlement as defined in Act on Banks, Art. 22, subparagraphs (3) and (4),

> d) Crimes as defined in Combating Smuggling Act, which carry imprisonment as punishment,
> e) Crimes as defined in Act on Protection of Cultural and Natural Substances, Arts. 68 and 74.
> (7) No one may listen and record the communication through telecommunication of another person except under the principles and procedures as determined in this Article.

The commonality of both articles of the TCPC are the following safeguards of the articles while resorting to the relevant measures, guaranteeing the protection of the right to private and family life in a democratic society. In order to invoke the measures envisaged in both articles;

- There must be a proper investigation launched upon a suspicion of a crime,
- There must be strong grounds of suspicion indicating that the crime has been committed,
- There must be no other possibility to obtain evidence,
- On the condition that above-mentioned three criteria are met, then a judge must decide to apply the measure set out in the said Articles.

Under Article 38/6 of the Turkish Constitution, "*Findings obtained through illegal methods shall not be considered evidence*". Pursuant to this provision, Article 206/2(a) of the TCPC reads that "*(2) The request of presentation of any evidence shall be denied …: a) if the evidence is unlawfully obtained*". Article 217/2 of the Code explicitly enhances the same principle as follows: "*the charged crime may be proven by using all kinds of legally obtained evidence*". As a natural and legal result of the afore-mentioned provisions, Article 289(i) thereof strictly prohibits basing the judgments on the evidence obtained with illegal methods by classifying such situations as "*absolute violation of the law*".

With those fundamental provisions in mind, the law enforcement which gathers digital evidence without any regard for the procedures stipulated under Articles 134 and 135 of the TCPC commits various crimes under the TPC. Likewise, any acquisition of data bypassing the aforementioned procedures cannot be used as evidence before a court of law under Article 38/6 of the Turkish Constitution, as well as Article 206/2(a) and Article 289(i) of the TCPC. When interpreted along with the Constitutional Court's decision[8] that "*digital data cannot be claimed to show the absolute reality*", the law governing the acquisition of digital evidence and its presentation before a court is considerably restrictive, thereby obliges the law enforcement to conduct its investigation in a very delicate and transparent manner.

[8] Decision No. 2013/7800

3. A Real Case-Based Study

Delving deep into the matter through a real case would shed further light on how sophisticated the commission of cybercrimes could become and how jointly we must well-appreciate and implement the aforementioned articles.

For the purposes of personal data protection, I have not identified the names and other identifying personal information in the case study examined below. I am approached by a client of mine and told that he was being charged for cyber offences under article 243 and 245 of the TPC. My client is a UKASH seller, a UK-based electronic money system that allowed users to exchange their cash for a secure code to make payments online. After careful examination of the indictment issued against my client, I inferred that, although he is accused of unlawfully accessing a data processing system and of improperly using credit card, he is the actual victim of cybercrime whose perpetrator penetrated into my client's data processing system and thereby exercised an electronic fraud using the client's data processing systems.

To expand the story a little further, the cybercriminal hacks the complainant B's Facebook account and, masquerading as herself, requests via the Facebook medium the credit card information of the complainant A who is a close friend of the complainant B. Confiding in that the request comes from a close friend, the complainant A sends her credit card information to the cybercriminal.

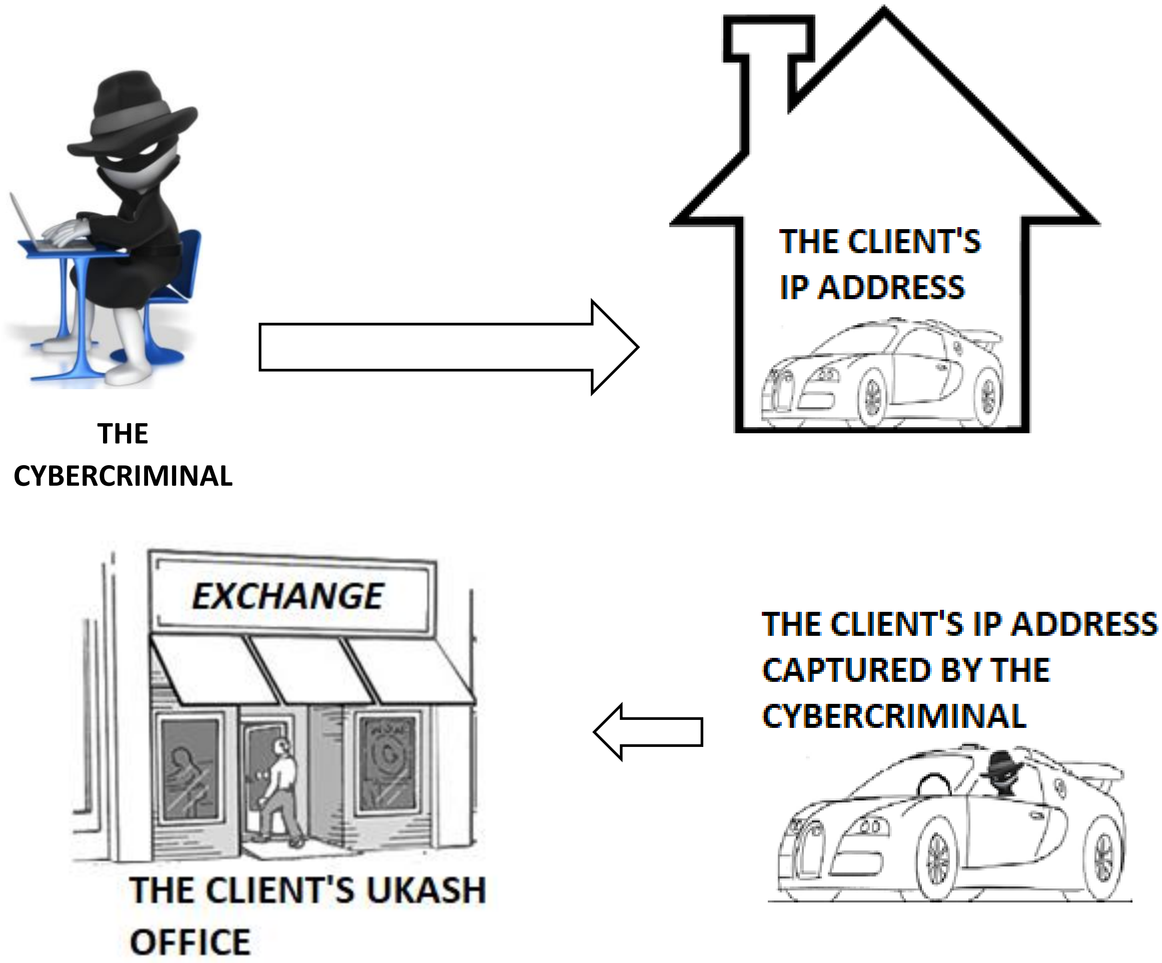
THE COMPLAINANT B'S CREDIT CARD

THE CYBERCRIMINAL

THE COMPLAINANT B'S FACEBOOK ACCOUNT

In order to legitimize the usage of the credit card and to conceal the payments which will be made later on using the credit card, the cybercriminal purchases a UKASH from my client and pays the price for the UKASH using the credit card. The purchase of the UKASH enables the cybercriminal to make payments online or transfer money through a secure code which corresponds to some amount of electronic money. Thus, the online shopping centers which accept the payment in the form of UKASH would only see some code encrypted in a secure manner so that they do not identify who makes the payment. In short, they don't know who the cybercriminal is, neither does the law enforcement.

The downside of all these delicate steps taken by the cybercriminal is that he realizes all these transactions using an IP address specifically registered in the name of a company owned by my client. In other words, the cybercriminal hacks my client's data processing system and illegally seizes the IP address exclusively used by my client. Using this IP address, the cybercriminal first captures the complainant B's Facebook account. Using the same IP address, the cybercriminal then purchases UKASH from my client. Using an analogy, the cybercriminal steals some Turkish liras by a car owned by my client and then goes to the client's exchange office with the same car to change the Turkish lira with Euros.


THE CYBERCRIMINAL
THE CLIENT'S IP ADDRESS
EXCHANGE
THE CLIENT'S UKASH OFFICE
THE CLIENT'S IP ADDRESS CAPTURED BY THE CYBERCRIMINAL

Moving on the fact that the complainant B's Facebook account was captured using the client's IP address and that the payment for UKASH were made from the complainant A's credit card using the same IP address, the law enforcement have come up to the conclusion that the cybercriminal is my client. However, this wrong conclusion fails to take into consideration the facts that my client hasn't gained profit from this crime and that a cybercriminal who managed to capture the complainant's Facebook account could have easily captured my client's IP address as well and frame up him for this illegal activities.

Regardless of who really is the perpetrator, it is certain that the offences laid out under Articles 243 and 245 of the TPC were committed. The data processing system of the complainant B were unlawfully entered, thus the conditions stipulated under Article 243 of the TPC for the formation of the offence are met. Likewise, the complainant A's credit card were possessed and used without A's consent, thus the conditions stipulated under Article 245 of the TPC for the formation of the offence are met as well.

4. Conclusion

As is seen in the aforementioned case study, cybercrimes can be committed using ever-sophisticated cyber methods and capabilities. As is the case in the study, attribution is one of the biggest challenges of combatting cybercrimes for law enforcement authorities. Conducting e-commerce and other cyberspace activity in a safe and strongly encrypted manner is of utmost importance. On the other hand, the growing misuse of the same legitimate anonymity and encryption services and tools for illegal purposes pose significant impediment for the law enforcement to detection, investigation and prosecution of cybercriminals.

Besides, in the cyber domain, boundaries between the traditional crimes and cyber-facilitated crimes blur, so do the actual boundaries between states. Given the immediacy and speed with which a cyber offence can be committed, the actual perpetrator might be at any point in the world. This phenomenon leads us to appreciate the vitality of cooperation and coordination between states in combatting crimes in cyber domain. Existing frameworks, programmes and tools are often too slow and bureaucratic to allow for a timely and effective response. In that regard, instant coordination between law enforcement of the respective states would enable them to address the threat stemming from cyber domain in a timely, conclusive and efficient manner.[9]

[9] Internet Organised Crime Threat Assessment (IOCTA), s. 12.