

Gökçe

The Resolution

February 2018

Issue

03

Fighting Cybercrime



Highlights of this issue

Investigation and Prosecution
Phases in Cybercrimes

For further information please contact us at contact@gokce.av.tr

All Rights Reserved

FIGHTING CYBERCRIME

While the flow of life is getting easier with technology, cybercrimes cause material and spiritual losses are increasing day by day. Recently, we faced such cybercrime in the opening ceremony of the Winter Olympics. In the ceremony, a cyber-attack took place and in addition to the interruption of the wireless network in the stadium, the official web site of the organization could be used barely 12 hours after the ceremony.

According to Section of Fighting Cybercrime in Istanbul, cybercrimes mean the crimes committed by using an information system and aimed to the security of an information system and/or its related data and/or its user. The distinctive feature of a cybercrime from the other crimes is that it cannot be committed without an information system.

The types of crimes related to cybercrimes in Turkey are regulated under Turkish Criminal Code and are subject to ex officio investigation. Such types of crimes defined in Turkish Criminal Code are entering the information system (art.243), blocking or disrupting the system, destroying or changing the data (art.244) and abusing of the bank or credit cards (art.245). In case to commit the defined cybercrime provides benefits for any legal entity, then the security measures prescribed in Turkish Criminal Code for legal entities, as laid down in TCC article 246, might be taken. Additionally, the crime of recording of personal data (art.135), the crime of sharing or retaining personal data unlawfully (art.136 and 137) and the crime of destruction of data (art. 138) are among the crimes defined in the field of information technologies.



INVESTIGATION AND PROSECUTION PHASES IN CYBERCRIMES

In the investigations subject to cybercrimes in Turkey, a forensic science study is conducted. In addition, during the investigation / prosecution phase, the activity of data exchange is conducted between the Information Technologies and Communications Authority; which is supervisor agency formally organize the telecommunication sector in Turkey, and the Chief Public Prosecutor or the Court to ensure the objective causality between act and perpetrator and attribution of the crime to the perpetrator . Cyber experts are consulted when the Chief Public Prosecutor or the Court considers such consultancy is necessary.

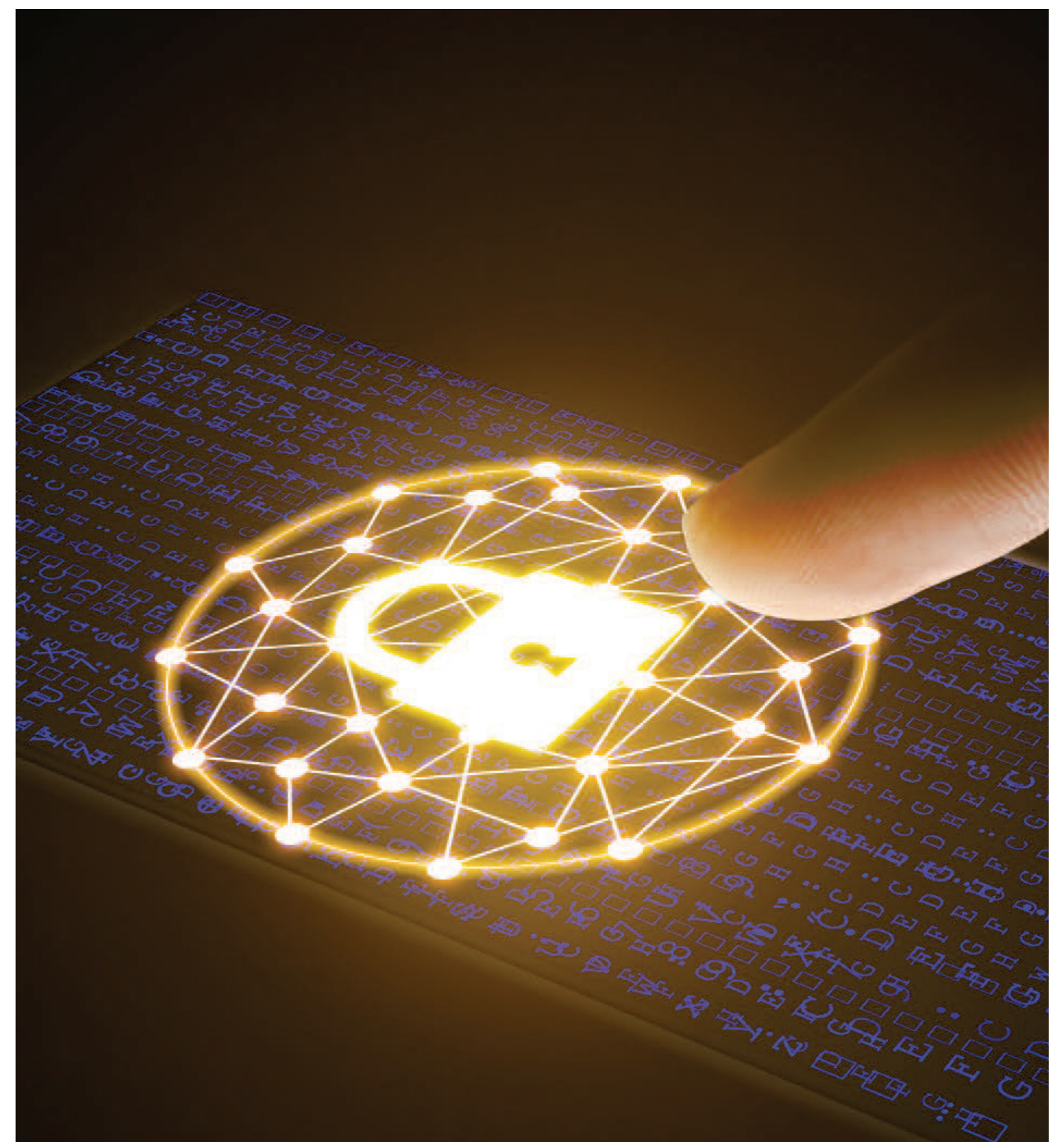
The phase of forensic investigation is composed of different stages and can be sorted as follows: Preparation, first intervention to digital evidences, forensic copy (image) retrieval, examination and reporting. The forensic copy (image) retrieval phase is one of the most critical stages. In the process of image retrieval from the computer used as a crime tool, it must be ensured that the received images (evidences) are not modified.

For the security of the investigation, it must be proved that, the images taken by the algorithm called Hash Algorithm, have not been modified after the retrieval. In this regard, the credibility of the evidence is ensured in the investigation. Also, at this stage, before the image retrieval operation, a software or hardware called write block which does not corrupt the integrity of the evidences should be used. Write block is a hardware or software for reading the retrieved data (evidence) without writing on the evidence to be retrieved. Therefore, since the evidence is not corrupted even in the examination stage, a definite result is obtained.

After the image retrieval operation, the examination is carried out by the experts and the experts must have detailed information regarding the crime, the perpetrator and the subject of the crime. At this stage, the expert will isolate the elements of the crime (malicious software, photographs, documents, source codes etc.) from the digital world one by one and determine any kind of data that can be used to establish the causal relation between the perpetrator and the act and to charge the perpetrator with the crime. After the completion of the expert's examination, the examined evidences and the conclusion will be reported to the Chief Public Prosecutor or to the relevant Court. Thus, the most critical stage to prove the cybercrime is completed. Essentially the Chief Public Prosecutor and the Courts leave their places to the experts and even to the software for the cybercrimes and other digital disputes.

In order to retrieve the data, a remote intervention is required to our personal devices. The most common method used for such intervention is viruses. Please keep in mind that using up-to-date software is beneficial to get rid of the viruses since the viruses are created as computer codes, updating obliges the viruses to rewrite.

Nowadays, since the states cannot provide a proper protection to the victims of cybercrimes, insurance companies have begun to work on giving new services under the name of "cyber risk insurance". In this type of insurance, the insurer provides data loss assurance, warranty for the compensation claims arising from the data violation and guarantee for the loss of profits arising from the business intervention insurance. Which basis will be taken into account is still an ongoing debate when the judicial authorities will decide in respect of the disputes between the parties.



Answers. Not theories.

Gokce Attorney Partnership

Editors:



Doç. Dr. Ali Paslı
ali.pasli@gokce.av.tr



Aslihan Kayhan
aslihan.kayhan@gokce.av.tr



Ece Özkan
ece.ozkan@gokce.av.tr



Mehmet Topluyıldız
mehmet.topluyildiz@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at contact@gokce.av.tr
0 212 352 88 33

The Resolution olara is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to receive further information, please contact Gokce Attorney Partnership. No content provided in The Resolution can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Resolution was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.

For further information please contact us at contact@gokce.av.tr