EXPERIENCE OF FOREIGN COUNTRIES IN THE COLLECTION, STORAGE AND USE OF ELECTRONIC EVIDENCE

Anvarov Olimjon Rustam ugli
Personnel Centre for Cybersecurity of
The Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: *The article dwells on advanced practices of foreign countries in the storage, transportation, use and collection of electronic evidence, such as electronic documents, video and audio, electronic correspondence, electronic message, the Internet, electronic disks and flash drives are highlighted.*

Keywords: *electronic signatures, electronic seals or electronic time stamps, digital evidence, data privacy, flexibility of data, collection of electronic evidence.*

ОПЫТ ЗАРУБЕЖНЫХ СТРАН ПО СБОРУ, ХРАНЕНИЮ И ИСПОЛЬЗОВАНИЮ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Анваров Олимжон Рустам Угли
Сотрудник Центр Кибербезопасности МВД РУ

Аннотация: *В статье рассматривается передовой опыт зарубежных стран по хранению, транспортировке, использованию и сбору электронных доказательств, таких как электронные документы, видео и аудио, электронная переписка, электронное сообщение, Интернет, электронные диски и флешки.*

Ключевые слова: *электронные подписи, электронные печати или электронные отметки времени, цифровые доказательства, конфиденциальность данных, гибкость данных, сбор электронных доказательств.*

Electronic evidence. “Electronic evidence” means any evidence derived from data contained in or produced by any device, the functioning of which depends on a

software program or data stored on or transmitted over a computer system or network.

Metadata. "Metadata" refers to electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times.

Trust service "Trust service" means an electronic service which consists of:

a. the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

b. the creation, verification and validation of certificates for website authentication; or

c. the preservation of electronic signatures, seals or certificates related to those services.[1]

In US practice, digital evidence should only be verified by specially trained experts. Because given the variety of electronic devices in use today and the rate at which they change, it can be very difficult for local law enforcement to track them down.

Devices should be turned off immediately and batteries removed if possible. Turning off the phone preserves the cellular device's location and call logs and prevents phone usage that could change data on the phone. Also, if the device is turned on, remote kill commands can be used without the knowledge of the investigator. Some phones have an automatic timer that allows the phone to receive updates (updates) that can corrupt data, so it's best to take the battery out.

If the device cannot be turned off, digital devices should be placed in special bags, placed on airplane mode, or turned off Wi-Fi, Bluetooth, or other communication systems, and placed in antistatic packaging such as paper bags or envelopes and cartons. The device should not be stored in plastic as it may conduct static electricity or allow condensation or moisture to accumulate.

[1] Electronic evidence in civil and administrative proceedings. Council of Europe. 2019. P. 6-7.

When submitting digital devices to the laboratory, the researcher should specify the type of information requested, such as phone numbers and cell phone call history, emails, computer documents, messages, or images.

On-Site: Devices may be seized once the scene has been secured and legal authority to seize evidence has been established. Any passwords, codes or PINs must be obtained from participants, if possible. Electronic devices are tested in a special laboratory.

Vietnam's Criminal Procedure Code (2015) recognises "electronic data" as a source of evidence. The same law has specific rules for acquiring, storing, preserving, copying, restoring, and displaying electronic data. The findings of expert examinations may be used to explain and present digital evidence. The Law on E-Transactions (2005) provides for the legal validity of data messages. This study has found that Bangladesh, Bhutan, Brunei, Sri Lanka, and Vietnam have enacted specific laws to facilitate the use of digital evidence in criminal cases, and these laws are a valuable reference for jurisdictions contemplating similar reforms. Cambodia and the Maldives have draft laws which are still going through the legislative process. All countries, except the Maldives, have legal provisions to facilitate the admission of expert opinions as evidence. Such evidence can assist the court in understanding the probative value of digital evidence. When material digital evidence is located outside the jurisdiction, additional efforts are needed to request and obtain such evidence. Most of the beneficiary countries reported making requests to overseas technology companies such as Facebook to provide account subscriber information. Without any legal compulsion for the companies to co-operate, such requests do not often yield immediate or helpful results.[2]

Today, in many countries there are problems with the use of electronic evidence storage. One of the main reasons for this is that electronic devices are not assembled by experts who understand the use of electronic devices during the initial collection of evidence. As a result, cases of inadvertent removal of electronic evidence from the device are not uncommon. As a solution to this problem, the

[2] The use of digital evidence in prosecutions in Asia. Report of Interpol. Norwegia, 2022. P. 3

country's Code of Criminal Procedure and other regulations should clearly define the storage, collection and use of electronic evidence.

Overall, the events which significantly left an impact on the contemporary legal landscape called for quick actions which led to the many different legal frameworks concerning data and cybercrimes. Although none of these legal frameworks specifically addresses e-evidence, they are still applied for the handling of such. Consequently, this could result in an unclarity where the numerous legal provisions, principles and norms becomes relevant during an investigation. Therefore, the complex rules may become hard to grasp and comply with, leading to a legal uncertainty that affects data privacy. From a technological perspective, the contemporary legal frameworks are in need of improvements and a greater consideration to the flexibility of data. In order to better accommodate to the challenges at hand, an EU regulation concerning the handling of e-evidence would significantly improve the respect for data privacy during the prevention of cybercrimes. Considering the discrepancy between data privacy and the need to effectively counter cybercrimes, it may seem like there is a separate attitude towards the collection of electronic evidence and for the protection of privacy. Despite the strong interconnectivity between the areas, one side of the discourse would advocate for a stronger protection of data, while the other side pushes for an extended mandate to mirror, trace and collect data for the purpose of preventing crimes. Nevertheless, both sides of the argument must be reconciliated to facilitate a legal framework which encourages the collection of evidence while also respecting privacy rights.[3]

References:

1. Electronic evidence in civil and administrative proceedings. Council of Europe. 2019. P. 6-7.
2. The use of digital evidence in prosecutions in Asia. Report of Interpol. Norwegia, 2022. P. 3

[3] The Collection of Electronic Evidence in the Prevention of Cybercrimes. Wandee Setthapirom. Sweden, 2021. P. 33-34

3. The Collection of Electronic Evidence in the Prevention of Cybercrimes. Wandee Setthapirom. Sweden, 2021. P. 33-34