Cybercrime, victimization and the role of e-evidence for victims' protection

Prof. Dobrinka Chankova, PhD
South-West University - Blagoevgrad, BULGARIA
Member of COST Action 18121

17th International Symposium of the World Society of Victimology, San Sebastian, 5-9 June 2022

Online world

Background information

- The massive use of Internet, social networks and digital media has encouraged criminal practices.
- Overall crime has almost doubled as a result of the inclusion of cyber offences in the data.
- Statistically, according to a European survey, one in 10 people now is a victim of fraud or other online offences.
- Unlike many traditional crimes, the victims of cyber offences are drawn from all ages, all social backgrounds and all areas of the world, meaning that no one who uses a computer regularly can feel safe.

Background information

- For the purposes of this paper a small-scale survey was launched among random population in Bulgaria in May 2022.
- The results are in compliance with the information generally distributed.
- The people become victims of online crime even more often- more than 20 % report they have been victimized in different ways.
- More than 70% say their sense of victimhood is growing.
- Over 90% believe that not enough is being done by the state and institutions to protect them in cyberspace.

Background information

- The term *cybercrime* refers to a variety of crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, games consoles and smart phones.
- *Cyber-enacted crimes* can only be committed on the internet - stealing confidential information that's stored online, for example.
- Other definitions used – *computer crime*, *e-crime*, *net crime*, etc.

Background information

- Cybercrime covers a wide range of offences including:
- bank and credit card fraud,
- hacking,
- sexual harassment,
- sextortion,
- bullying,
- copyright infringement,
- child pornography and even so-called romance scams where people are persuaded to part with thousands of Euro/pounds/dollars by people posing as their lovers online.

Online crime peculiarities

- Committing crimes online allows someone to hide their identity and location.
- Again, unlike with traditional crime, criminals can target their victims from miles away and clear their bank accounts without ever coming into contact with them.
- The victims are sometimes not even aware they have been targeted until they realise their savings have been raided, by which point it is often too late.

Online crime peculiarities

- In addition to the financial losses, fraud and other online offences leave people feeling violated, lacking in confidence and ashamed.
- They blame themselves for not doing more for effective protection.
- Cyber attacks can cause economic damage and erode public trust in online services, like energy, water and transport networks and are a problem for national security. (Recently hackers caused great problems to Bulgarian Posts)
- The statistics also alarm that the youngsters (15–24 year old) who are active Internet users are more likely to be exposed to cybercrime than older age groups.

Online crime peculiarities

- Cybercrime has become a leading concern in the legal community as criminals continue to spread troublesome viruses, access private business/financial information, commit cyber espionage and cyber terrorism, spread different variations of malware, execute property and identity theft, spread malicious online content, and invade computer system processes that may threaten or cause danger to the government or its citizens.
- So, due to its seriousness, it is not difficult to predict that cybercrime could lead into war.

Online crime peculiarities

Response

- The legal community devise laws that victims can consult to protect their privacy and rights.
- The aim is to cultivate a healthier, fraud-free online environment and to control and prevent such inconveniences, damage and loss as well as punish those who are responsible for the crimes committed.

Response

- A good example is Title 18 of the **U.S. Criminal code,** incriminating:
- Interception and disclosure of wire, oral, or electronic communications
- Unlawful access to stored communications
- Fraud and related activity in connection with computers
- Activities relating to material involving the sexual exploitation of minors, etc.
- Similar provisions could be found in many countries.

Response

- The European Union adopted **Directive 2013/40/EU on attacks against information systems.**
- All offences in the directive, and other definitions and procedural institutions are also in the **Council of Europe's Convention of Cybercrime (2001).**
- In 2006 entered in force the **Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems**
- On 12 May 2022 the **Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence** was opened for signature. It is already signed by 18 European countries, incl. Bulgaria, but also by Chile, Japan, US, etc.
- However, such provisions are never sufficient if the crime is not proved.

Investigation problems

- With many cyber criminals based overseas, it makes it extremely difficult for the police to investigate and bring the perpetrators to justice.
- In addition, just a fraction of offences are reported to the police because victims either feel embarrassed or believe little can be done to catch those responsible.
- Cybercriminals use developing countries where laws against cybercrime are weak or sometimes nonexistent in order to evade detection and prosecution from law enforcement.
- The ability to commit crime online demonstrates the need for policing to adapt and transform to tackle the cyber problems.

Evidencing

- These inevitably challenge the very **concept of evidencing.**
- Traditionally, evidence was gathered in physical form.
- After the invention of photography it became a common practice to take photographs at the crime scene and present the photographs along with other evidence.

Evidencing

- With the digital revolution and following the usage of electronic devices in almost all aspects of life it became necessary to allow evidence extracted from electronic devices, especially with electronic storage capacity, for use in judicial proceedings.
- We call such evidence **‘electronic evidence’.**
- While there is a difference with digital evidence, both are accepted terms in the scientific community and for this lecture they will be used interchangeably.

Evidencing

Definitions

- There are many different definitions of “Electronic/Digital Evidence”, each of them highlighting some, but not all, essential features.
- Usually as *e-evidence* are considered any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (Carrier, 2006, Casey, 2011).

Definitions

- *Electronic Evidence* is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device (Evidence Project).
- *Electronic evidence* is evidence that can be collected in electronic form (Council of Europe Convention on Cybercrime).
- *E-evidence* is the information stored or transmitted in binary form that may be relied on in court (U.S. Department of Justice).

Definitions

- In general though, most definitions seem to summarize that electronic evidence is digital data that can be used to help establish (or refute) whether a crime has been committed.
- No doubt, this kind of evidence is essential (and sometimes the only one) to prove committing online crime and protect victims' interests.
- Hence, the electronic evidence gathering process is of utmost importance in many cases.

Different sources of e-evidence

Different sources of e-evidence

- There are numerous sources of digital evidence and each requires a different process for gathering that evidence as well as different tools and methods for capturing it.
- It is not just the personal computer, laptop, mobile phone or Internet that provide sources of digital evidence, any piece of digital technology that processes or stores digital data could be used to commit a crime.
- The device and information it contains may store relevant digital evidence for proving or disproving a suspected offence.

Different sources of e-evidence

- It is vital that responders are able to identify and correctly seize potential sources of digital evidence.
- An example of the types of digital devices encountered by a digital forensic practitioner include, but are not limited to the following:
- Computers – such as Personal Computers (PC's), laptops, servers or even game consoles
- Storage devices – Compact Discs, Digitally Versatile Discs, removable data storage drives (USB thumb drives) and memory cards
- Handheld devices - mobile (smart) phones, digital cameras, satellite navigation systems
- Network devices like hubs, switches, routers and wireless access points, etc.

Basic characteristics of digital evidence

- **It's invisible to the untrained eye.** Electronic evidence is often retrieved from places known or accessible only to experts.
- **It may need to be interpreted by a specialist.** In many cases information gained requires thorough analysis to uncover properties assuring the information is valid from judicial point of view.

Basic characteristics of digital evidence

- **It's highly volatile.** A powered electronic device modifies its state every time a specific event happens. Lack of power or a system overwriting old data with new data requires us to preserve electronic evidence as soon as possible.
- **It may be altered or destroyed through normal use.** Devices constantly change the state of memory – allocating it for programs automatically, swapping it to disk or writing chunks of it to a disk file on user request.

Basic characteristics of digital evidence

- This characteristic calls for using appropriate tools and techniques from the very moment of identification of the evidence as relevant for an investigation.
- **It can be copied without limits**. This property allows many specialists to work on the same evidence at the same time in different places. It also enables the possibility of presenting the evidence as-is in the court of law along with the specialist witness report.

E-evidence life cycle

- Usually, the e-evidence life cycle is presented in the following algorithm:
- *Evidence Identification*: this is the step consisting of examining/studying the crime scene in order to preserve, as much as possible, the original state of the digital/electronic devices that are going to be acquired.

E-evidence life cycle

- *Evidence Handling*: this is the step where it is defined which specific standard procedures are to be followed, based on the kind of device being handled.
- *Evidence Classification*: this is the step consisting of identifying the main features and the status of the device, taking notes about Case ID, Evidence ID, Seizure place/date/made by/ Evidence type, picture, status, etc.

E-evidence life cycle

- *Evidence Acquisition*: the forensics specialist must take care of the potential digital evidence in order to preserve its integrity during the following processes till the presentation before a Court.
- *Evidence Analysis*: this is a process heavily affected by the kind of case under investigation, the type of evidence to be handled and the features related to each of the evidence to be examined (e.g. installed operating system, type of file system, etc.).

E-evidence life cycle

- *Evidence Reporting*: this is one of the most critical steps. After the completion of identification, acquisition and analysis activities, digital evidence specialists have to complete their job producing a report with all the activities carried out and the outcome achieved. The report must contain all details to allow the specialists to testify before a Court only relying on that document.

E-evidence life cycle

- To assist law enforcement agencies and prosecutorial offices, a series of guides dealing with electronic/digital evidence has been developed to address the complete investigation process.
- This process expands from the crime scene through analysis and finally into the courtroom.

E-evidence life cycle

Principles

- There are **5 main principles** that establish a basis for all dealings with electronic evidence.
- These principles were adopted as part of the European Union and the Council of Europe project to develop a ‘seizure of e-evidence’ guide and are used internationally.
- **Principle 1 – Data Integrity**
- No action taken should change electronic devices or media, which may subsequently be relied upon in court.
- When handling electronic devices and data, they must not be changed, either in relation to hardware or software. The person in charge is responsible for the integrity of the material recovered from the scene and thus for initiating a forensic chain of custody.

Principles

- **Principle 2 – Audit Trail**
- An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved.
- An independent third party should be able to examine those actions and achieve the same result.
- **Principle 3 – Specialist Support**
- If it is assumed that electronic evidence may be found in the course of an operation, the person in charge should notify specialists/external advisers in time.
- A specialist should have:
- Necessary expertise and experience in the field,
- Necessary investigative knowledge,

Principles

- Necessary knowledge of the matter at hand,
- Necessary legal knowledge,
- Appropriate communication skills (for both oral and written explanations)
- Appropriate language skills.
- **Principle 4 - Appropriate Training**
- First responders must be appropriately trained to be able to search for and seize electronic evidence if no experts are available at the scene.
- They should explain the relevance and implications of his/her actions.

Principles

- **Principle 5 – Legality**
- The person and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to.

Advantages and inconveniences of electronic evidence

Advantages and inconveniences of electronic evidence

- A major issue is the **reliability.**
- While some believe that its objectivity and precision make it more reliable and therefore they favour its use, others think that the lack of means to verify its authenticity make it more vulnerable and therefore less reliable than traditional evidence, considering it an inconvenience for its use and admissibility.

Advantages and inconveniences of electronic evidence

- Electronic evidence offers information that is exact, complete, clear, precise, true, objective and neutral, given that it comes from an electronic element, in which there is no subjectivity whatsoever, when comparing it to, for example, the declarations made by witnesses that can always be contradicted.
- Moreover, it gives access to information which until now was impossible to obtain, such as everything that is contained in electronic devices.

Advantages and inconveniences of electronic evidence

- On several occasions, electronic evidence is considered as essential to solving certain crimes, because **this evidence was the only existing proof,** therefore turning out to be very useful.
- Another advantage is the **ease and rapidity** in collecting and using it as well as its conservation and storage.
- However, the establishment of legal value on this type of evidence could be a difficulty due to the **existing ignorance about data processing procedures** and of the interpretation of prosecutorial law in this respect.
- This difficulty is generated by the **lack of suitable and systematic regulation** as well as the **lack of homogenous jurisprudence**.

Advantages and inconveniences of electronic evidence

- There is a fear about the **vulnerability** and ease with which this evidence **can be manipulated,** given its high degree of **volatility**, which is one of the inconveniences when proving its authenticity.
- Also, it is technical evidence that is not understood by judges and prosecutors, it is hard to explain and out of this feeling comes the rejection of using it in court.

Legal issues

Legal issues

- **The admissibility of e-evidence in criminal proceedings is a crucial point, indeed.**
- Laws regarding admissibility of evidence differ between countries.
- In certain countries there are defined rules as to admissibility of evidence in legal proceedings, while in other countries admissibility is flexible.

Legal issues

- **Evidence rules vary considerably** even amongst countries with similar legal traditions.
- In certain countries, traditional investigative powers might be general enough to apply to electronic evidence, while in other countries traditional procedural laws might not cover specific issues regarding electronic evidence, making it necessary to have additional legislation.

Legal issues

- Furthermore, national legislation and policies may negatively affect an investigation. For example, privacy and data protection laws in some EU Member States may prevent the collection of evidence, and varied data retention periods across jurisdictions may complicate investigations.
- Legislation may not sufficiently address the realities of modern investigations, especially when it comes to evolving new technologies.

Legal issues

A suggestion

- It seems, **a common internationally accepted framework** for handling, use and exchange of e-evidence in prosecution of online crime is more than needed.
- It will help to improve the efficiency of investigations and judicial procedures while maintaining adequate safeguards aimed at protecting relevant fundamental human rights (both of victim and offender) and respecting clear standards of conduct.

A suggestion

- This **uniform regulation should address** more specifically:
- Common definitions, concepts and standards;
- Guidelines for collection, preservation and use of e-evidence;
- Specific investigative measures;
- Admissibility based on mutual trust;
- Transfer of electronic evidence;
- Effective cross-border cooperation.

A suggestion

- This is the way to ensure also **proportionality between the protection of privacy** (both of victim and offender) and **legitimate crime prevention and control**.
- An adequate level of data protection could be achieved as well as of data security, in particular safeguards against the alteration of electronic evidence, during the life cycle of e-evidence.

Latest developments in Europe

Latest developments

- To make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists, the European Commission proposed in 2018 new rules in the form of a Regulation and a Directive, which will:

Latest developments

- **create a European Production Order:**
- this will allow a judicial authority in one Member State to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another Member State, which will be obliged to respond within **10 days**, and within **6 hours** in cases of emergency (compared to up to 120 days for the existing European Investigation Order or an average of 10 months for a Mutual Legal Assistance procedure)

Latest developments

- **create a European Preservation Order:**
- this will allow a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order;
- **include strong safeguards:**
- the new rules guarantee strong protection of fundamental rights, including safeguards for the right to protection of personal data.
- The service providers and persons whose data is being sought will benefit from various safeguards and be entitled to legal remedies;

Latest developments

- **oblige service providers to designate a legal representative in the Union:**
- to ensure that all providers that offer services in the Union are subject to the same obligations, even if their headquarters are in a third country, they are required to designate a legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders.
- **provide legal certainty for businesses and service providers:**
- whereas today law enforcement authorities often depend on the good will of service providers to hand them the evidence they need, in the future, applying the same rules for access to all service providers will improve legal certainty and clarity.

Latest developments

- **Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment was approved**
- The directive updates the legal framework, removing obstacles to operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.
- **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online**

Latest developments in Bulgaria

- Bulgaria is a country with well developed and widely used online services.
- Hence, the probability of being victimized while doing something in the cyberspace is high.
- Some preventive measures have been taken on different institutional levels.
- A new Bill for amendments of the Penal Code envisaging raising of sanctions for cybercrimes has been enacted recently.
- There is ongoing information campaign.
- However, a lot remain to be done.

Conclusions

- The Internet and technology have penetrated nearly every aspect of our daily lives. This has created many positive conveniences, but also provides criminals with opportunities to reach new victims.
- Technology is constantly evolving and criminals are always finding new ways to manipulate it, so we must always remain vigilant and adopt new safety measures on a regular basis.

Conclusions

- Everyone of us needs to take greater responsibility for protecting themselves from cyber hackers.
- Partnerships with industry and academia will allow to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked.
- Good offline social networks were a protective factor against cybercrime victimization, especially among females.

Conclusions

- Proper education, sharing of advanced knowledge and promoting the exchange of experience and best practices between police officers, judges, prosecutors and defense lawyers who deal with criminal cases involving e-evidence, is essential.
- Cross-border cooperation should be encouraged.
- New procedural safeguards and standards for handling of e-evidence should be provided in order to resolve common problems and achieve justice for victims in the online world.

References

References

- Carrier, B. (2006). *Hypothesis-Based Approach to Digital Forensic Investigations*. Center for Education and Research in Information Assurance and Security. Purdue University
- Casey, E. (2011). *Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet*. Elsevier, Third Edition
- Chankova, D. (2018).Towards New European Regulation for Handling Electronic Evidence, (in co-authorship), *US-China Law Review*, March 2018, Vol.15, No. 3, pp. 121-129

References

- The Evidence Project: Bridging the Gap in the Exchange of Digital Evidence Across Europe, by Maria Angela Biasiotti, Mattia Epifani, Fabrizio Turchi. *In: Proceedings of 10th Intl. Conference on Systematic Approaches to Digital Forensic Engineering* (SADFE 2015)
- Council of Europe. *Convention on Cybercrime*, CETS N. 185, Budapest, 23 November 2001

References

- U.S. Department of Justice, Office of Justice Programs, National Institute of Justice: *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004) 1st ed.
- *Electronic evidence: a basic guide for First Responders, ENISA (2014)*
- Council of Europe (2013). *Electronic Evidence Guide*
- Biasiotti, M. A proposed electronic evidence exchange across the European Union, *Digital Evidence and Electronic Signature Law Review*, 14 (2017)

Relevant websites

- https://www.coe.int/en/web/cybercrime/home
- https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
- https://www.europeanlawinstitute.eu/projects-publications/current-projects-upcoming-projects-and-other-activities/current-projects/admissibility-of-e-evidence/

Thank you for your kind attention!

chankova@law.swu.bg