Committee: Legal Committee

Issue: Addressing the issues related to ''e-evidence''

Student Officer: Fragiskos Nistikakis

Position: Co-Chair

PERSONAL INTRODUCTION

My name is Fragiskos Nistikakis and as I am currently 16 years old, I am attending the 11th class of the German School of Athens (DSA). It is my honor to serve as one of your Co-Chairs in the Legal Committee (GA6) in this year's ACG-MUN Conference.

Before I proceed with the rest of the study guide, I would like to congratulate all delegates and participants on deciding to join the 4th ACG-MUN Conference. By attending such a Conference, you will have the irreplaceable opportunity to engage yourselves in pending issues affecting people all around the globe. Despite the fact, that MUN might seem challenging or even intimidating sometimes, I would like to assure you that the outcome of your work is going to be pleasing and rewarding. Apart from the unique experiences, you are going to improve essential skills like public speaking, working in a group or debating, while you are going to be able to experience long lasting friendships with attendees from all around the world.

As the Student Officer Team of the Legal Committee, we are going to do everything possible to create a friendly environment, where fruitful debate can take place. We are all looking forward to working with you towards sustainable solutions that will ensure a more equal world for all. When it comes to the context of the study guide, it refers to the first topic of the GA6 agenda, namely the question of addressing the issues related to "e-evidence". At this point, I would like to mention the fact that the following study guide is only going to provide you with a clear overlook of the issue. Following its close examination, you are all expected and kindly asked to conduct further research on the matter and on your countries policy on your own, so that you are going to be able to represent it at the debate that will take place during the conference.

If you have any further question on the issue, the conference or the study guide in general, feel free to contact me on my personal e-mail (fragiskos2004@gmail). I would be more than happy to provide you with any kind of clarification or guidance on the topic at hand.

I am really looking forward to virtually meeting you all!

Best of luck,

FragiskosNistikakis

TOPIC INTRODUCTION

The so-called digitalization, that clearly describes our modern society, is clearly redefining every aspect of our lives. When it comes to criminal activity, it is no secret that technology gets used more than ever before, thus forcing authorities to become reliant on e-evidence.

Mobile devices that often contain personal information such as call history, digital photographs or even text messages, could potentially be seen as useful digital sources of legal evidence that could be legally examined or taken into consideration by courts or other authorities. Electronic evidence refers to various types of data in an electronic form. Such are typically stored on servers of online service providers and are divided into two categories, namely content data and non-content data. Content data are the aforementioned e-mails, text messages, photographs and videos, while non-context online data could be subscriber data or even traffic information regarding any kind of online account.

The use of e-evidence as legal evidence is a matter of respecting the importance of Law Enforcement and could be seen as a "legal tool" of authorities, when it comes to the investigation and prosecution of serious crimes in order to achieve legal certainty.

Due to the complex nature of the issue at hand and due to the fact that half of the investigations today include the use of electronic evidence, it is of great importance that all nations create and introduce new legislation to protect and promote the use of e-evidence, while respecting the right of privacy of citizens.

In order to understand such complexity, one must take the new challenges that are created due to digital crime into consideration. Traditionally, evidence could be found in documents or fingerprint for instance, while evidence tampering was not that easily carried out. On the other hand, e-evidence is not physical, but kept online. Therefore, apart from the fact that criminals are indeed able to obtain a series of "barriers" prohibiting local authorities from accessing it, it may also be stored in different member nations, thus proving that e-evidence is a new type of evidence that requires different legislation.

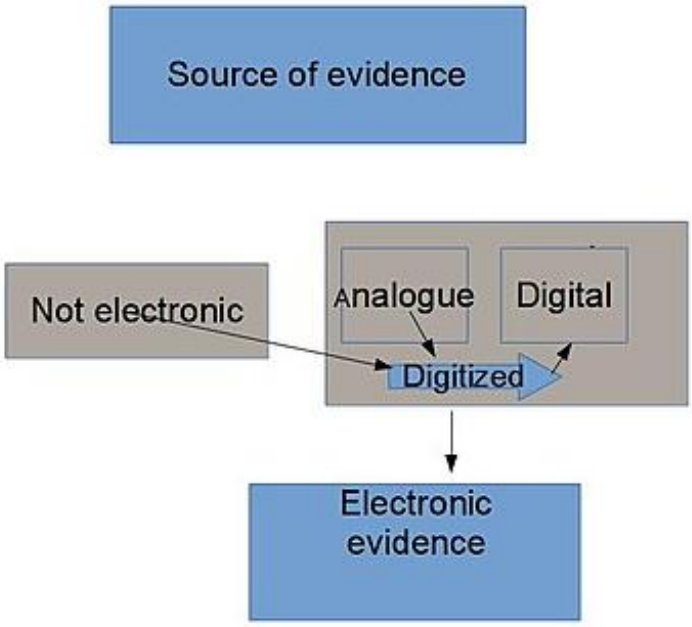

Figure 1: E-evidence and it'shearsay

DEFINITION OF KEY TERMS

E-evidence[1]

"Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial [...] Digital Evidence is information of probative value that is stored or transmitted in binary form".

Law Enforcement Agencies (LEA)

As a law Enforcement Agency could be described any kind of agency enforcing the law, including a special, local, state or even a federal organization. LEA's could also be found at an international level, since the term Law Enforcement Agencies could describe an international organization enforcing the law, such as the Europol or the Interpol.

Judicial Authorities[2]

[1]"Admissibility of Electronic Evidence: an Indian Perspective." *Forensic Research & Criminology International Journal*, 14 Mar. 2017, medcraveonline.com/FRCIJ/admissibility-of-electronic-evidence-an-indian-perspective.html.
[2]"Law Insider." *Law Insider*, www.lawinsider.com/dictionary/judicial-authority.

"Judicial Authority means any court, arbitrator, special master, receiver, tribunalor similar body of any kind (including any Governmental Authority exercising judicial powers or functions of any kind)".

Legal Certainty[3]

"In the context of legal modernity, the principle of legal certainty—the idea that the law must be sufficiently clear to provide those subjects to legal norms with the means to regulate their own conduct and to protect against the arbitrary exercise of public power—has operated as a foundational rule of law value".

Case Law[4]

"Case law is law that is based on judicial decisions rather than law based on constitutions, statutes, or regulations. Case law concerns unique disputes resolved by courts using the concrete facts of a case".

Right to Privacy[5]

"Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech".

BACKGROUND INFORMATION

Already existing legislation

It is logical that policymakers are not able to formulate policies applying to all cases. In order to resolve any kind of ambiguities of the current legal framework, tribunals have to take the so-called Case law into consideration. Case law is the collection of past legal decisions made, obtained and reached by courts on similar cases that were previously been trialed. Such judicial interpretations of the law are distinguished based on already existing legal codes enacted by local legislative bodies. Therefore, courts are partly bounded to their previous decisions and should formally follow the same law applicable recorded to prior cases that have been decided. Despite the fact that Case Law plays a major role in some judicial systems, legal courts are not prohibited from following past verdicts due to the fact that law sometimes proves to be unable to reflect the way that societies are constantly changing.

Due to the fact that e-evidence differs from traditional evidence to a large extent, e-evidence has not been covered or directly mentioned by law yet. Due to the

[3]"The Shifting Meaning of Legal Certainty." *SpringerLink*, link.springer.com/chapter/10.1007/978-981-10-0114-7_1.
[4]"Case Law." *LII / Legal Information Institute*, www.law.cornell.edu/wex/case_law.
[5]"Privacy and Human Rights - Overview." *Global Internet Liberty Campaign*, gilc.org/privacy/survey/intro.html.

fact that evidence is more reliable and not that easily distorted, courts still take e-evidence based on the already existing case law into consideration, so that similar facts and principles may be yielded and respected. However, as experts have already commented on the matter, courts and other judicial bodies cannot rely on the Case law alone.

The use of e-evidence on a National Level

Obtaining and evaluating e-evidence on a national level is not that challenging. Local Law Enforcement Agencies (LAEs) are able to gather digital information if needed. Apart from that, due to the fact that such e-evidence is stored within the nation's territory, there is no doubt that it is accessible as well.

Formally, individuals are indeed allowed to bring digital evidence as normal evidence to any legal court. However, in order for the court to take the aforementioned e-evidence into consideration, some specific guidelines must be fulfilled beforehand. By setting such, the court succeeds in protecting fundamental human rights, like the right to the privacy, or in proving the authenticity of the evidence provided.

The use of e-evidence on an International Level

When it comes to obtaining and evaluating e-evidence on an International Level, new guidelines and procedures must be followed. At this point, we are not referring to digital evidence stored to a member state's own territory, but to a foreign one. Therefore, getting access to e-evidence is not always a straightforward procedure for authorities and LEAs, since the majority of service provides store data in a variety of servers that may be located in several countries.

The issue of Cross border Law / Cross Border Access

As it was previously mentioned, accessing e-evidence on an international level is much more difficult and it is considered to be a long-lasting procedure, as judicial authorities are forced to undergo lengthy and complicated courses of action in order to obtain access to it.

But apart from that, there are further problems that arise on the matter at hand. The current legislation leaves many service providers and legal authorities in legal uncertainty as to which data requests they have to fulfill. Bearing in mind, that there is no international legislation defining which requests should indeed be deemed valid, it is left up to the authorities to decide that.

The "Microsoft Ireland case"

The "Microsoft Ireland case" was highlighted by the issue of the court's jurisdiction over cross-border access to e-evidence. The case dates back to an initiative

of a judge of the United States District Court for the Southern District that demanded that the court would grand access to specific e-mails that would later on be used as normal evidence. Due to the fact that the aforementioned communication content was stored on one of the company's servers in Ireland, Microsoft refused to comply questioning the court's jurisdiction over data stored on another state's territory. However, such objection was later on overturned and the court granted access to the aforementioned e-evidence files.

Data protection and privacy aspects of cross-border access to e-evidence

While constantly exchanging data, the issue of data protection and privacy arises. In order for parties, Legal Enforcement Agencies and Judicial Authorities to access e-evidence in a lawful manner, a procedure respecting the fundamental human rights needs to be followed.

More specifically, the principle of necessity should always be taken into consideration. While permitting access to third parties, one must always take into account the impact on the rights of the person whose data are being requested.

It is important to take into consideration that this pertains to personal messages, videos, documents etc. Privacy rights protect citizens from governmental overreach and protect them from illegal governmental collection of personal information. The right of individuals to be protected against unwarranted and illegal invasion of their privacy from the collection, maintenance or use of personal information, should be respected.

Personal data shouldn't be obtained in the form of e-evidence, unless it is considered to be obligatory or necessary for purposes of prevention, investigation and prosecution of crimes. An issue with many privacy rights violations is that an individual may be completely unaware of them, which of course should be the case. Enabling LEAs to access e-evidence in the most efficient manner is a priority, however the right to privacy should never be undermined.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

The United Kingdom (UK)

The United Kingdom (UK) has announced the obtainment of measures to speed up the processes of exchanging Cross Border Access e-evidence, thus clearly showing UK's commitment and acknowledgment of the issue's importance.

The UK government proceeded with signing the "UK-US Bilateral Access Agreement", which will ensure the legal access of both the signatories Law Enforcement Agencies (LEAs), by ensuring that both parties will have the authorization to access useful data directly, instead of following the aforementioned long lasting procedures.

The United States of America (USA)

Similarly, the United States of America (USA) are interested in creating a legal framework facilitating the easiest and most beneficial way of exchanging e-evidence data as well.

By following the U.S. CLOUD Act, a legal agreement that allows foreign countries to enter into so-called "exclusive agreements" with the US government in order to grand access to communication content stored in US territory, the USA intends to respond to the converse problem that foreign countries may face, when it comes to accessing data held by American service providers.

Germany

On the other hand, the government of Germany remains one of the few opposing to such agreements. Germany claims that allowing foreign governments to directly obtain e-evidence on criminal suspects without requiring judicial approval first, is a measure that is going to be easily abused by certain governments in the near future, thus undermining fundamental human rights. Based on that idea, the government of Germany is concerned that speeding up cross-border access to digital evidence poses national security threats to nations and makes them vulnerable. Nevertheless, Germany's representatives support that member states need more efficient ways of accessing criminal evidence without endangering national security.

European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor, also known as EDPS, is an independent data protection authority with the primary goal to monitor and further ensure the protection of personal data and privacy.

Apart from that, the European Data Protection Supervisor is also responsible for monitoring new technologies that may affect the protection or personal information. Due to the fact that EDPS is conducted by experts on the matter, it is also appropriate for the organization to take an advisory role to EU bodies or governments by simple providing them with guidance on interpretating data protection law or by simply working towards the protection of personal information.

Sharing Electronic Resources and Laws on Crime (SHERLOC)

Sharing Electronic Resources and Laws on Crime, the SHERLOC, is an initiative of the United Nations Office on Drugs and Crime (UNODC) in order to promote the dissemination of data and information. It is a comprehensive database, where e-evidence is gathered and later on published. It allows users to see how member states are currently tackling crime both operationally and in their courts. The SHERLOC portal has proven to be an important legal "tool" for police investigators, prosecutor or even

judges, while it could also be described as an awareness-raising tool for the public and media.

The International Criminal Police Organization (INTERPOL)

The International Criminal Police Organization (INTERPOL) is an inter-governmental organization that facilitates worldwide police cooperation and crime control.

Apart from providing a secure network for constant cooperation among nations, INTERPOL allows nations to access databases gathering real time e-evidence as well. INTERPOL is currently conducting efforts to help Law Enforcement Agencies throughout the globe to leverage technological advantage for their own benefit. By doing so, INTERPOL is able to gather, analyze and provide nations with digital evidence as an effort to keep local police task forces up to date.

TIMELINE OF EVENTS

Date	Description of event
7 September 1923	The international Criminal Police Organization (INTERPOL) was founded.
17 January 2004	The European Data Protection Supervisor was formed.
1 July 2004	The Convention on Cybercrime was adopted.
27 April 2016	The basis of protection of natural persons with regard to the processing of personal data and on the free movement of such, have been set by the EU.
1 January 2016	The 17 Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable Development were adopted.
14 July 2016	The “Microsoft Ireland case” took place. One of the fist cases where a court’s jurisdiction over cross-border access to e-evidence was questioned.
17 April 2018	The Regulation on European Production and Preservation Order for electronic evidence in criminal matters proposed the two aforementioned legislative proposals.

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime is the first international treaty on crimes committed and carried out via the internet or other computer networks.

The main objective of the Convention at hand, is to create a common criminal policy aimed at the protection of our modern society against cybercrime, especially when it comes to adopting the appropriate legislation and fostering international co-operation. It is no secret that the Budapest Convention has played a key role, when it comes to setting the basis for the creation of domestic legislation on cybercrime and electronic evidence worldwide and domestic investigations on such legislation.

Regulation on European Production and Preservation Order for electronic evidence in criminal matters

The Regulation on European Production and Preservation Order for electronic evidence in criminal matters is consisted by two legislative proposal seeking to address barriers in cross-border access to e-evidence in criminal investigations.

First and foremost, the European production order would allow local judicial authorities to request e-evidence directly from foreign service providers rather than local governments. Furthermore, such European preservation order would also obligate a service provider to preserve specific data, which the aforementioned authority may have previously requested. Service providers offering services and e-evidence within the EU would be requested to appoint a so-called legal representative in order to ensure the efficient gathering of e-evidence.

Sustainable Development Goalsnumber 16 (SDGs)

Sustainable Development goal number 16 aims to promote inclusive societies, provide access to justice and build effective and accountable institutions at all levels in order to archive sustainable development.

While promoting access to justice, one must promote access to evidence, both physical and electronic, as well. Without evidence, access to justice will never be achieved.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Due to the importance of the issue and its ongoing developing nature, the UN and member states have remained generally active on the issues related to e-evidence.

First and foremost, the existence of the Case law could be seen as a previous attempt to regulate e-evidence. Even though, courts are indeed able to be guided

based on previous legal decision though case law, it is no secret that case law has failed to promote cooperation among nations and to protect fundamental rights threatened by e-evidence, due to the fact case law is not applicable to all cases.

Last but not least, nations have proceeded in obtaining joint agreements that will allegedly improve the issue of access to cross-border evidence. However, a lot of nations have expressed their concerns and have opposed from the aforementioned agreements. It has been claimed that ensuring that foreign Law Enforcement Agency are indeed able to access e-evidence beyond their territory, certain human rights are undermined and not respected, while national security threats due to vulnerability have been created. Bearing in mind, that e-evidence is typically stored in a verity of territories, such agreements must be obtained by the majority of nations in order to be reliable.

More specifically, in order to make it easier and faster for law enforcement and judicial authorities to obtain e-evidence stored in foreign territory, a series of measures have already been obtained. First and foremost, efforts have been made in order to legally allow authorities to access and obtain e-evidence directly from the service provider or its legal representative rather than the local government. In order to solve the issue of privacy, new rules and other kinds of safeguards have been introduced, while most of the countries have introduced laws legally binding service providers to cooperate with foreign LEAs, since LEAs often depended on the good will of service providers, postponing the whole procedure.

POSSIBLE SOLUTIONS

First and foremost, in order to reach comprehensive and sustainable resolutions, all of the aforementioned problems must be taken into consideration. As it was previously mentioned judicial authorities are currently forced to undergo lengthy and complicated courses of actions and procedures in order to obtain access to any kind of e-evidence stored in a foreign server or territory. Such procedures postpone the process of trials and are considered a barrier to legal certainty. Many policymakers and experts on the matter have proposed that new legislations, allowing authorities to grand access to e-evidence directly from service providers rather than local governments, must be introduced. However, many member states, have expressed their concern on the issue, since allowing foreign governments to access e-evidence that easily and without the evolvement of the local governments might endanger national security. Apart from that, the fact that the current legislation leaves service providers in legal uncertainty as to which data requests they have to fulfill, undoubtedly proves that new legal frameworks and standard legislation must be introduced. For example, delegates can introduce detailed legislation proposals establishing legal frameworks, where authorities are going to be able to obtain access

to e-evidence directly from the service providers, only in a case of an emergency, where legal procedures must be fulfilled as quick as possible.

Furthermore, the right to privacy should be taken into consideration as well. Individuals should be protected against unwarranted and illegal invasions of their privacy. Therefore, legal standards should guarantee that e-evidence may only be obtained, when it is considered to be obligatory or necessary for purposes of prevention, investigation etc. of crimes. In order to achieve the aforementioned goal, the committee may introduce a so-called UN body with the responsibility to monitor such requests. The European Data Protection Supervisor (EDPS) may be taken as an example. However, the fact that it operates on an EU level, rather than an international, should be taken into consideration.

Last but not least, it has been concluded that most of the previous attempts to solve the issues have failed to do so, due to the fact that such measures have been obtained by certain member states, rather than collectively. Bearing in mind, that e-evidence may be stored in multiple nations, measures should be obtained by the majority of them, in order to be deemed as effective, thus proving that establishing a joint legal framework is of great importance.

BIBLIOGRAPHY

"Admissibility of Electronic Evidence: an Indian Perspective." *Forensic Research & Criminology International Journal*, 14 Mar. 2017, medcraveonline.com/FRCIJ/admissibility-of-electronic-evidence-an-indian-perspective.html.

"Better Access to E-evidence to Fight Crime." *Consilium*, www.consilium.europa.eu/en/policies/e-evidence/#.

"E-evidence - Cross-border Access to Electronic Evidence." *European Commission - European Commission*, 2 May 2019, ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

"E-evidence." *Migration and Home Affairs - European Commission*, 23 May 2017, ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

"E-evidence." *Migration and Home Affairs - European Commission*, 23 May 2017, ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

European Telecommunications Network Operators' Association, etno.eu/datas/positions-papers/2018/ETNO%20position%20paper%20on%20improving%20cross-border%20access%20to%20electronic%20evidence%20in%20criminal%20matters.pdf.

Evidence, s.evidenceproject.eu/p/e/v/evidence-ga-608185-d2-1-410.pdf.

"Law Insider." *Law Insider*, www.lawinsider.com/dictionary/judicial-authority.

Welcome to the United Nations, www.un.org/sc/ctc/wp-content/uploads/2020/01/Battlefield_Evidence_Final.pdf.

"About." *European Data Protection Supervisor - European Data Protection Supervisor*, 11 Nov. 2016, edps.europa.eu/about-edps_en.

arno.uvt.nl/show.cgi?fid=148179#page=30&zoom=100,109,622.

"Case Law." *LII / Legal Information Institute*, www.law.cornell.edu/wex/case_law.

"E- Evidence: Admissibility of Email As Evidence." *Indian Legal Solution*, 16 Jan. 2021, indianlegalsolution.com/e-evidence-admissibility-of-email-as-evidence/.

"EU Governments Approve Draft Rules on Sharing 'e-evidence'." *Financial Times*, 7 Dec. 2018, www.ft.com/content/63a6105a-fa24-11e8-af46-2022a0b02a6c.

Media. "Electronic Evidence and Its Admissibility in Court." *Welcome to the Signaturit Blog*, blog.signaturit.com/en/electronic-evidence-and-its-admissibility-in-court.

rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

"US and UK Sign Bilateral E-Evidence Agreement - Eucrim." *Homepage - Eucrim*, eucrim.eu/news/us-and-uk-sign-bilateral-e-evidence-agreement/.

"Privacy and Human Rights - Overview." *Global Internet Liberty Campaign*, gilc.org/privacy/survey/intro.html.

"E-evidence - Cross-border Access to Electronic Evidence." *European Commission - European Commission*, 2 May 2019, ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

"The Right to Privacy." *Carmichael, Ellis & Brock PLLC - Criminal Defense Attorneys | Alexandria, VA*, www.carmichaellegal.com/the-right-to-privacy.

Graphs

Admissibility of Electronic Evidence: an Indian Perspective." *Forensic Research & Criminology International Journal*, 14 Mar. 2017, medcraveonline.com/FRCIJ/admissibility-of-electronic-evidence-an-indian-perspective.html.