REVIEW ARTICLE

UDK: 343.98
DOI: 10.59245/ps.32.3.2
Received for publication: January 2022

KRUNOSLAV ANTOLIŠ *

The Challenges of Collecting Digital Evidence Across Borders

Abstract

In the modern world, the use of ICT communication technologies has become an integral part of life. ICT infrastructure is the bearer of digital traces of both legal and illegal activities performed through it. However, for something to become digital evidence, it must be obtained by law and by a person authorised by law. Namely, the virtual infrastructure, especially the Internet and the new challenges brought to us by cloud architectue due to its physical positioning outside national borders, calls into question the legality of searching and collecting digital evidence outside national borders. This paper analyses the legal basis for collecting digital evidence in cyberspace internationally, such as the Council of Europe Convention on Cybercrime, the US Cloud Act, the Australian Decryption Act and the European GDPR. Although the Court of Justice of the European Union declared invalid the decision of the European Commission (EU) 2016/1250 on the adequacy of data protection provided through the EU-US Privacy Shield, experts must not stop looking for a solution to the apparent problem. The paper intends to support decision-makers in taking clear national positions regarding the above controversial legal norms and their mutual conflict. The paper compares the legal consequences of such collection, and the acceptability of such digital evidence, and such collection may also be associated with a breach of the privacy of a legal and private entity.

Keywords: *digital evidence, cross border access, legal standards, Internet, cloud.*

1. INTRODUCTION

"The new historical era of the global communication society determines new information and communication technologies at all levels of media communication. The future democratisation

* Associate Professor Antoliš Krunoslav, PhD, Ministry of the Interior of the Republic of Croatia, Police Academy – The First Croatian Police Officer, University of Applied Sciences in Criminal Investigation and Public Security, Av. Gojka Šuška 1, 10000 Zagreb, Croatia.

of any pluralistic democratic society should be viewed in the context of the constant progress of new media, and information and communication technology "(Plenković, Mustić, 2020:69). In the modern information age we live in, evidence of crimes is increasingly being collected through smartphones, gadgets, IoT, the Internet and the cloud. This is also the main reason why digital evidence has become crucial in almost all criminal investigations. But that does not mean that gathering such evidence is simple and effortless. Law enforcement agencies face, among other things, two major challenges in their investigations: jurisdiction and encryption.

Effective criminal investigations often depend on whether the investigating state is authorised under domestic law to obtain electronic data held by ISPs under its jurisdiction, including their subsidiaries outside national borders.

The jurisdiction of national legal frameworks is limited to a specific state territory, and our communication and use of data, due to the Internet, cloud computing and technological development, knows no national borders. A provider of cloud communication and computing platforms such as Skype, WhatsApp, Microsoft, Google and Dropbox will often store data in the user's country of residence, thus denying the national legal system its ability to operate legally.

Communication service providers who often have electronic evidence of certain crimes can have clients around the world and business offices and storage facilities in many different countries. As a result, ISPs and controlled data may be subject to the laws of multiple states. Conflicting legal obligations may arise when an ISP receives an order from a government requesting disclosure, but the rest of the government restricts the disclosure of the same information, although they can be vital to timely and effective criminal investigations.

2. LEGALITY OF COLLECTING DIGITAL EVIDENCE FROM THE INTERNET AND CLOUDS

Various forms of crime today rely on information and communication technologies, especially the Internet and the cloud. "Such crime, hidden from public view due to the secretive nature of its activities, is a major threat to European citizens, businesses and state institutions, and to the economy as a whole. The same was highlighted in the latest assessment of crime threats in the European Union (EU SOCTA for 2021)."[2] The EU seeks to address these problems by recognising them, describing them and conceptualising them through strategic approaches such as "EU Strategy for Combating Organized Crime 2021-2025 Brussels, from 14.4.2021."[3]

[2] Europol, Serious and Organized Crime Threat Assessment in the European Union for 2021 (EU SOCTA), 12 April 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment. EU SOCTA is a comprehensive analysis of the threat of organized crime, identifying high-priority areas, carried out by Europol every four years on the basis of contributions from Member States.

[3] EU Strategy for Combating Organized Crime 2021-2025 Brussels, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170

Criminal groups "exploit their large illicit earnings to infiltrate legal economies and public institutions. They do so, inter alia, through corruption, the violation of the rule of law and fundamental rights, and the undermining of people's right to security and their trust in public bodies, with the proceeds of crime not small and in the European Union amounting to EUR 139 billion for 2019[4], which accounts for 1% of the Union's gross domestic product.

One example of a criminal association is from 2020, when "in a joint investigation conducted with the support of Europol and Eurojust by French and Dutch authorities to break up the EncroChat encrypted telephone network, which was widely used by criminal networks. The EncroChat case has led to more than 1,800 arrests and more than 1,500 new investigations. More than 70 violent crimes were prevented, more than 28 tonnes of ingredients for narcotics were seized, and more than 80 suspects involved in organised crime and drug trafficking were arrested in Belgium and the Netherlands. More than 400 new investigations into high-risk organised crime groups have also been launched."[5]

The following example is related to the COVID-19 disease pandemic, when criminal groups used the pandemic to increase their illegal activities on the Internet.[6] EU governments have so far uncovered fraud attempts and fraudulent offers by fraudsters who intended to sell 1.1 billion vaccine doses for a total of € 15.4 billion.[7]

Due to all the above, it is necessary to "strengthen the co-operation between law enforcement agencies and judicial bodies. When it comes to criminal groups active in EU Member States, 65% of them have members of different nationalities.

By operating in different jurisdictions, criminal groups avoid detection and take advantage of differences in treatment under national law."[8]

The jurisdiction of national legal frameworks is limited to a specific state territory, and our communication and use of data, due to the Internet, cloud computing and technological development, knows no national borders. A provider of cloud-based communication and computing platforms such as Skype, WhatsApp, Microsoft, Google and Dropbox will often store data in the country where the user is not a resident, thus preventing the national legal system from being able to operate legally.

[4] Study on Mapping the Risk of Infiltration of Serious and Organized Crime into Legitimate Enterprises, March 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101

[5] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to tackle Organised Crime 2021-2025, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170

[6] In an international operation conducted from March to December 2020, with the support of Europol and the European Anti-Fraud Office (OLAF), law enforcement agencies seized almost 33 million counterfeit medical devices, including face masks, from 19 Member States and eight third countries. test and diagnostic kits, 8 tons of raw materials and 70,000 litres of disinfectants.

[7] Information provided by government bodies to OLAF. Law enforcement agencies work together with Europol and OLAF to prevent attempted fraud.

[8] Ibid p. 9.

Telecommunications service providers, who often have digital evidence of certain crimes, can have clients around the world and business offices and storage facilities in many different countries. As a result, ISPs and controlled data may be subject to the laws of multiple states. Conflicting legal obligations may arise when an ISP receives an order from a government requesting data and information, but other governments limit the disclosure of the same information, although they can be vital to timely and effective criminal investigations.

The existing international mutual legal assistance (MLA) system has become too slow and cumbersome for law enforcement officials to keep up with growing criminal activity online. The system of cross-border access to electronic evidence needs to be reformed; otherwise, states could launch their national initiatives for access to data, such as data localisation measures. Building a sustainable regime will require working on two fronts: first, to improve rather than abandon the existing international legal aid regime, and second, to establish an effective system among those willing to certain common multilateral legal solutions, such as the European Convention on Cybercrime and the Second Additional Protocol to the Convention on Enhanced Co-operation and Disclosure of Electronic Evidence, which allows authorities in different countries to access data under commonly accepted conditions.

Therefore, the key to success lies in the simple exchange of data and information and timely access to them while fully respecting fundamental rights, especially the protection of personal data.

Legislators have responded to these challenges by introducing new legal solutions, and examples of these solutions were: The Clarifying Lawful Overseas Use of Data Act CLOUD Act, the Australian Decryption Act, the Council of Europe Convention on Cybercrime, GDPR − which cares about privacy on electronic infrastructures, as well as many others. The public often ignores the consequences and dilemmas that ISP providers may face in criminal charges for non-compliance with legal frameworks, as penalties are high. For example, the penalty for non-compliance with the EU General Data Protection Regulation (GDPR) is up to € 20,000,000 or 4% of total annual world turnover in the previous financial year.

The European Union has provided law enforcement agencies with a large number of tools to facilitate the exchange of information, such as the Schengen Information System (SIS), the 2008 Prüm Framework, the Passenger Name Record (PNR), pre-submitted Passenger Information (API), which have proven to be key to detecting illegal activities and networks.

Europol, with its databases, also has an important role to play in the fight against crime through the EU Crime Information Centers, which supports police co-operation and information exchange and prepares a European Union report on the threat of serious and organised crime every four years (EU SOCTA).

There is also the European Multidisciplinary Platform against Crime (EMPACT), a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime. EMPACT is one of the key tools for implementing and strengthening action against organised crime structures in coordinated operations. Under EMPACT, Member States and their partners carry out more than 200 joint operational actions to fight crime each year.

Interpol is another key player in international co-operation in the fight against organised crime. Interpol's 18 databases contain more than 100 million records of prosecutions, including information on wanted criminals, suspected terrorists, fingerprints, stolen vehicles, stolen and lost travel documents, and weapons and firearms.

For example, the main international instrument for co-operation and mutual legal assistance in organised crime investigations is the United Nations Convention against Transnational Organized Crime (UNTOC)[9] and the United Nations Convention against Corruption (UNCAC), to which the EU and member states are signatories.

All the mentioned capacities and legal norms are necessary to monitor the progress in the field of ICT, the development and use of new adequate hardware and software for digital forensics of the Internet and clouds, and their legal application in data collection and interception and communications. For them, it is necessary to develop standard operating procedures (SOPs) for their application, which should serve to initiate the construction and establishment of a digital forensic laboratory. All of the above should be established to approach the targeted training and specialisations of students, selected from the lines of work, who need digital evidence from the Internet and the cloud to perform everyday tasks.

2. 1. Council of Europe Convention on Cybercrime

The Convention on Cybercrime (also called the "Budapest Convention") requires that each of the 66 countries that are signatories to the agreement must retain legal authority and force companies in their area to disclose stored electronic information under their control in accordance with applicable law, without exception, in relation to information held by the company in another country.

"As stated by the production order of Article 18 – PRODUCTION ORDER

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order:

a. to a person in the territory of a Party to provide certain computer data which that person possesses or controls, which are stored in a computer system or on a computer data storage medium, and

b. to a service provider offering its services in the territory of a Party to provide subscriber information relating to those services, which information the service provider owns or controls.

2. The powers and procedures referred to in this Article shall be in accordance with Articles 14 and 15 of this Convention.
3. For the purposes of this Article, the term "subscriber information" means all information in the form of computer data or in any other form held by a service provider, concerning a subscriber to his services, with the exception of traffic data or content, and on the basis of which information the following can be determined:

9 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to tackle Organised Crime 2021-2025, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170

a. the type of communication service used, the technical measures taken and the period of service provided;

b. the subscriber's identity, postal or geographical address, telephone number and other access number, and information for sending invoices and payment information, available on the basis of a subscription contract or agreement;

c. all other information about the place where the communication equipment is installed, available on the basis of a subscription contract or agreement".[10]

However, ISPs may also be subject to the laws of other countries that restrict the disclosure of certain types of data, either because the data is stored in another country or require action in another country to disclose it or because the data relates to other nationals.

If national laws are in conflict, civil servants may be forced to choose the laws that countries will follow, knowing that they may face the consequences of violating the laws of another country. Such conflicts pose serious problems for the information requested by the government and may interfere with important investigations.

Sometimes such problems of conflict of law can be resolved by applying for "mutual legal assistance" to another state, using a system of agreements called the "Mutual Legal Assistance Treaty" (MLAT). Still, this process has many steps and can take several months, depending on the country and complexity. This is certainly one of the reasons why "Mutual Legal Assistance" (MLA) is generally considered ineffective in obtaining electronic evidence, as the binding response time to requests is in the standard of six to 24 months. This negatively affects the government's positive commitment to protecting society and individuals from cybercrime and other crimes involving electronic evidence.

To overcome the challenge of jurisdiction and speed up the investigation process, local authorities have, over the past few years, begun seeking information relevant to their criminal investigations directly from service providers, regardless of data location, and some countries have enacted regulations that make such a process legitimate.

2.2. Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence

Efforts to find common legal norms for collecting digital evidence are also happening in the EU. They are very clearly articulated in the form of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, completed in Brussels on 25 November 2021 and sent for signature to EU member states and all non-EU countries. The EU has ratified the Convention on Cybercrime.

The protocol covers procedures for improving international co-operation between competent authorities and strengthening direct co-operation with telecommunications service providers and entities located in other countries. It also lays down procedures for emergency mutual assistance.

[10] CONVENTION ON CYBERCRIME, https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html

This text will complement the EU framework for access to e-evidence, which the EU institutions are currently discussing. Its advantage is that it has the potential to be applied worldwide. The Convention presently includes 66 States Parties, including 26 EU Member States, taking into account existing Council of Europe treaties on co-operation in criminal matters and other agreements and arrangements on co-operation between the Parties to the Convention.[11]

Therefore, due to all the above, it is of great importance for the Republic of Croatia to ratify the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence to strengthen its capacity to fight crime.

2.3. Regulation on the European supply order and the European order for the storage of electronic evidence in criminal matters

In today's information and communication technology world, it is important to prepare law enforcement and judicial authorities for the digital age. Special emphasis should be placed on access to digital traces and evidence "because some traces and evidence are no longer physical but digital. A new moment is the speed with which data can be transferred between jurisdictions or the possibility of hiding them by encryption. In addition, some instruments and measures to collect physical evidence are not yet fully adapted to the digital world. This can interfere with or slow down criminal investigations and prosecutions because data is not available or accessible in a timely manner."[12]

"Difficulties with cross-border access to electronic evidence prevent effective investigations and prosecutions of crimes in the EU. Judicial co-operation between public authorities is not sufficiently effective, as is direct co-operation between public authorities and service providers or direct access by public authorities to electronic evidence.

As a result, investigations are suspended, crimes go unpunished, victims are given less protection, and EU citizens feel less secure.

There are three problems in the impact assessment: cross-border access to electronic evidence under existing judicial co-operation procedures takes too long and therefore reduces the effectiveness of investigations and prosecutions; the ineffectiveness of public-private co-operation between service providers and public authorities prevents effective investigations and prosecutions; shortcomings in defining jurisdiction can prevent effective cross-border investigations and prosecutions."[13]

---

[11] Access to e-evidence: Council authorises member states to sign international agreement https://www.consilium.europa.eu/hr/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/

[12] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to tackle Organised Crime 2021-2025 https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170

[13] Proposal REGULATIONS OF THE EUROPEAN PARLIAMENT AND COUNCIL on the European production order and the European order for the preservation of electronic evidence in criminal matters SWD(2018)119/F1 – HR https://eur-lex.europa.eu/legal-content/HR/TXT/

In order to resolve this most efficiently, an EU Regulation has been drafted which introduces a "binding European delivery order and a European storage order. Both orders must be issued or certified by a judicial authority of a Member State. An order may be issued requesting the storage or delivery of data held by a service provider located in another State which is required as evidence in criminal investigations or criminal proceedings."[14]

"Such warrants may be issued if a similar measure is available for the same offence in a similar situation in the issuing Member State. Both orders can be delivered to providers of electronic communications services, social networks, online stores, other server accommodation service providers, and Internet infrastructure providers such as IP addresses and domain name registries or their legal representatives, if any. The European retention order, as well as the European delivery order, shall be addressed to a legal representative outside the jurisdiction of the issuing Member State for the retention of data until a subsequent request for such data is issued, for example, through mutual legal assistance channels or EINs between participating Member States."[15]

The overall objective is to ensure effective investigation and prosecution of criminal offences in the EU by improving cross-border access to electronic evidence through enhanced judicial co-operation in criminal matters and harmonisation of rules and procedures.

There are also three specific objectives: to reduce delays in cross-border access to electronic evidence; ensure cross-border access to electronic evidence where it does not currently exist; improve legal certainty, protection of fundamental rights, transparency and accountability.

"Unlike surveillance measures or data retention obligations laid down by law, which are not provided for in this Regulation, a European custody order is an order issued or certified by a judicial authority in a particular criminal proceeding following an individual assessment of proportionality and necessity in each case. Unlike a European warrant, it refers to certain known or unknown perpetrators of a crime that has already been committed. The European retention order allows the storage of only those data that are already stored at the time of receipt of the order but not access to data in the future after receipt of the European retention order."[16]

HTML/?uri=CELEX:52018PC0225&from=EN

[14] Proposal REGULATIONS OF THE EUROPEAN PARLIAMENT AND COUNCIL on the European production order and the European order for the preservation of electronic evidence in criminal matters SWD(2018)119/F1 - HR https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

[15] Inter-institutional course:2018/0108 (COD) https://data.consilium.europa.eu/doc/document/ST-8110-2018-INIT/hr/pdf

[16] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European production order and the European order for the preservation of electronic evidence in criminal matters https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=COM%3A2018%3A225%3AFIN

"Both orders can only be used in criminal proceedings, from the initial pre-investigation phase to the end of the proceedings by a verdict or other decision. Subscriber or access data orders may be issued for any criminal offence, and transaction or content delivery orders may be issued only for a criminal offence punishable by a maximum term of imprisonment of at least three years in the issuing State or for certain criminal offences mentioned in the proposal and if there is a specific link with electronic tools and criminal offences covered by the Terrorism Directive 2017/541/EU."[17]

"This Regulation provides investigative bodies with additional tools for obtaining electronic evidence without limiting the powers established by national law to bind service providers established or represented in their territory. If the service provider is established or represented in the same Member State, the competent authorities of that Member State shall apply national measures to bind the service provider.

The information requested in the European delivery order should be provided directly to the competent authorities without the involvement of the competent authorities in the Member State where the service provider is established or represented. The regulation also moves away from the location of data as a decisive connecting factor because data storage usually does not lead to control by the country in whose territory the data is stored. In most cases, storage is decided by the provider based on the business decision.

Furthermore, the Regulation also applies if service providers are not established or represented in the Union but provide services there.

Where the proposal refers to a service provider established and a representative in a Member State through an appointed legal representative, the appointment of a legal representative shall not create the establishment of a service provider for the purposes of this Regulation."[18]

The Regulation also provides a range of definitions, such as: "service provider", "establishment", "electronic evidence", "subscriber data", "access data", "transaction data", "content data", "Information system", "issuing State", "executing State", "executing authority", "emergencies".

As there are some differences from national legislation, perhaps the most interesting definition is the following: electronic evidence is "evidence stored in electronic form stored by the service provider or stored on his behalf at the time of receipt of the delivery or storage order confirmation, consisting of stored subscriber data, access data, transaction data, and content data."[19]

[17] Ibid p. 3.

[18] Inter-institutional course:2018/0108 (COD) https://data.consilium.europa.eu/doc/document/ST-8110-2018-INIT/hr/pdf

[19] Ibid p.38.

2.4. Data retention

Regarding access to "digital evidence and investigative clues, Member States have established frameworks for data retention. Efforts to speed up the digitisation of law enforcement and judicial authorities are also part of this, and all Member States should participate in the digital e-evidence exchange system (eEDES)."[20].

The key legal act related to data retention in the Republic of Croatia is the "Decree on National Security Obligations of the Republic of Croatia for Legal and Natural Persons in Telecommunications, of 15 May 2003. This Decree regulates the obligations of legal and natural persons that dispose of public telecommunication networks and provide public telecommunications services and access services relating to the function of secret surveillance of telecommunications in the Republic of Croatia. This Regulation transposes into the legal order of the Republic of Croatia Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data obtained or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006)".[21] The following are the specific obligations arising under this Regulation that explicitly oblige actors to store and intercept data.

"Legal and natural persons who have a public telecommunications network and provide public telecommunications and access services within the meaning of this Regulation are telecommunications operators, network operators, service providers, access providers and other legal and natural persons specified by law.

Legal and natural persons referred to in this Regulation are obliged to ensure and maintain at their own expense the function of secret surveillance of telecommunications services, activities and traffic they perform."[22]

The secret surveillance function must enable the full application of secret data collection measures: secret surveillance of communications content, secret surveillance of telecommunications traffic data, secret surveillance of user locations and secret surveillance of international telecommunications connections.

The secret surveillance function referred to in this Regulation shall be performed by installing and maintaining appropriate technical equipment and software in the telecommunications system of legal and natural persons referred to in this Regulation by installing communication lines to the Operational Technical Center for Telecommunications Supervision (hereinafter: OTC) - for permanent and direct access to facilities, communication

[20] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,TO THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy for Combating Organized Crime for the period 2021-2025.https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?from=EN&uri=CELEX%3A52021DC0170

[21] REGULATION ON OBLIGATIONS IN THE AREA OF NATIONAL SECURITY OF THE REPUBLIC OF CROATIA FOR LEGAL AND NATURAL PERSONS IN TELECOMMUNICATIONS https://narodne-novine.nn.hr/clanci/sluzbeni/2003_05_83_1013.html

[22] Ibid p. 5.

lines and technical equipment and ensuring conditions for independent implementation of secret data collection measures using appropriate technical interfaces.

Legal and natural persons from this Regulation must keep data on telecommunication traffic realised within and through their telecommunication capacities, and the data must be available to OTC for the period of the last 12 months through the prescribed technical interface. The stored data should also contain data generated as a result of the established telecommunication connection in the event that it is not answered.

3. PRIVACY ON THE INTERNET AND CLOUD

One, if not the most prominent example in which the required data is stored on foreign servers is Microsoft Ireland. The case began in December 2013, when a U.S. court ordered Microsoft to hand over data belonging to a Microsoft email account in Ireland. The service provider challenged the court order based on arguments about jurisdiction and sovereignty, which resulted in a legal battle between the Ministry of Justice and Microsoft, which ended before the Supreme Court in 2017.

However, before the Supreme Court could rule on the matter, the U.S. Congress passed the CLOUD Act in March 2018, which now allows U.S. (Law Enforcement Agency) LEAs to request data from U.S. service providers even if that data is stored on servers abroad.

The United States has enacted the CLOUD Act, which speeds up access to electronic information held by global ISP providers based in the United States.

Law on Clarification of the Law on Legal Use of Data Abroad or "Cloud Law". The Cloud Act allows the United States to enter into executive agreements with other countries that meet certain criteria, such as respect for the rule of law, in resolving conflicts of law. For serious crime investigations, ISPs may qualify for qualified, legitimate electronic data orders issued by another state.

The CLOUD Act clarified that U.S. law required that providers subject to U.S. jurisdiction disclose data that is responsive to valid U.S. legal processes, regardless of where the company stores the data. CLOUD requires that ISPs under U.S. jurisdiction must disclose information that complies with U.S. law, regardless of where the company stores the data.

The CLOUD Act requires that orders from foreign governments that are subject to an executive agreement must not intentionally target individuals or individuals in the United States in the United States. A foreign government is free to negotiate similar restrictions that would prevent the United States from using the orders that are the subject of the agreement to target its citizens or residents. The U.S. and other countries may continue to use their existing legal process to seek information outside of the CLOUD law, but in such circumstances, they may still face a conflict of laws.

At the same time, the court proceedings required by the plaintiff state under the CLOUD Act do not have to comply with legal requirements in the United States. Instead, court proceedings must comply with the requirements of domestic law for the requested information.

When operating under the CLOUD Act, foreign authorities may use their domestic legal procedures directly to service providers in accordance with their law, and service providers may disclose responsible information directly to foreign authorities.

The CLOUD Act has not changed or expanded the historical scope of orders issued under U.S. law, i.e., random or group data collection is not permitted.

The CLOUD Act applies in accordance with the following definitions: 18 U.S.C. § 2510 (15) ("electronic communications service" means any service which provides users with the possibility of sending or receiving wireless or electronic communications); ID card. § 2711 (2) ("Remote computer services" means the provision of computer storage and data processing services via an electronic communication system to the public).

These definitions include companies such as email providers, mobile phone companies, social media platforms, and cloud storage services. They don't involve a business just because they have a certain interaction with the Internet, like certain e-commerce sites.

These definitions are in line with Article 1c. of the Budapest Convention, which includes "any public or private body which provides its users with the possibility of communication via a computer system" and "any other entity that processes or stores computer data on behalf of such a communication service or a user of such a service".

Even if LEAs gain access to the data, for example, either by downloading a mobile phone or requesting data from a service provider, the growing popularity of encryption technology prevents LEAs from understanding the data. Data in encrypted format only reveals encrypted information.

A real-life example should help to understand these challenges better. A federal judge has asked Apple to assist the Federal Bureau of Investigation in providing reasonable technical assistance to unlock an encrypted iPhone belonging to a San Bernard terrorist attacker since December 2015. Apple refused, fearing such help could set a precedent and harm technology security encryption in the coming years. Finally, the FBI managed to unlock the iPhone without Apple's help, which is why the case did not continue.

Another example relates to encrypted communication. In a two-year investigation that was present in the media, in 2013, the FBI removed the Black Market Silk Road forum, which allowed the trade in drugs and other inadequate goods on the Internet. The Silk Road owes its success to a combination of anonymity and encryption. It was a hidden service in Darknet, a computer network that uses a cryptographic communication protocol, making it difficult to enforce the law to locate the site's server, its administrators, and its users. Finally, the server was in Iceland at the time and was seized after a successful request for U.S. mutual legal assistance.

Concerns about the privacy created by the GDPR in the territory of the EU in the application of the CLOUD law are also reflected in the fact that ISPs may inform search account holders in accordance with a US court order under the Preserved Communications Act unless an independent judge did not issue a guarantee of orders. A protection order relating to all provisions of the Preserved Communication Act (and not just orders under the Cloud Act) will be issued when an independent judge determines that there is reason to

believe that a court order notice could lead to an adverse outcome (1) physical security of the individual; (2) escape from persecution; (3) destruction or manipulation of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardise the investigation or unduly delay the trial. In line with U.S. Department of Justice policy, such orders must generally be limited to one year.

It is important to know how the EU-US Privacy Shield actually works. "The program is managed by the US Department of Commerce's International Trade Directorate and is an online 'self-certification' system for US entities wishing to provide services to European companies, whose services include the transfer of personal data from the EU to the US. Self-certification involves self-evaluation of its processes according to set parameters accompanied by automated services set in the system (for example, automated issuance of Privacy Policy based on entered data) and, finally, payment of an annual fee for issuing certificates to eligible entities, depending on their annual income.[23]

One needs to be familiar with its historical development to understand how the UE-US Privacy Shiel came into being. In October 2015, the European Court of Justice annulled a previous framework called International Principles for the Protection of Privacy in a judgment that later became known as "Schrems I". Shortly after this decision, the European Commission and the US Government began talks on a new framework, and on February 2, 2016, they reached a political agreement. The European Commission has published a draft "adequacy decision", declaring the principles equal to the protection offered by EU law. The Article 29 Data Protection Working Group issued an opinion on 13 April 2016 stating that Privacy Shield offers major improvements compared to the Safe Harbor decisions but that three main points of concern remain. They relate to deleting data, collecting huge amounts of data and clarifying the new ombudsman mechanism.

The European Data Protection Supervisor issued an opinion on 30 May 2016 stating that "the Privacy Shield, as it stands, is not strong enough to withstand future legal review before the [European] Court". On 8 July 2016, representatives of the EU Member States (Article 31 Committee) approved the final EU-US version of the Privacy Shield, which paved the way for a decision by the Commission.

The European Commission adopted the framework on 12 July 2016 and entered into force on the same day. On January 25, 2017, U.S. President Donald Trump signed an executive order entitled "Improving Public Safety", stating that U.S. privacy protections will not be extended beyond U.S. citizens or residents: Agencies will, to the extent that in accordance with applicable law, ensure that their privacy policies exclude persons who are not citizens of the United States or lawful permanent residents from the protection of the Privacy Act with respect to personal data.

The president of the USA, Joe Biden, revoked this executive order on January 20, 2021, which is related to the USA only. The European Commission has stated that: The US Privacy

[23] The EU court declared the EU-US Privacy Shield invalid! Where is our personal data really? https://lidermedia.hr/sto-i-kako/sud-eu-a-proglasio-nevazecim-eu-us-stit-privatnosti-gdje-su-stvarno-nasi-osobni-podaci-132479

Act has never offered Europeans the right to data protection. The Commission has agreed on two additional instruments to ensure the proper protection of EU citizens' data when transferred to the US: the EU-US Privacy Shield, which does not rely on protection under the US Privacy Act; the EU-US umbrella agreement, which enters into force on 1 February (2017).

To finalise this agreement, the U.S. Congress passed a new law in 2017, the U.S. Justice Act, which extends the benefits of the U.S. Privacy Act to Europeans and gives them access to U.S. courts." The commission said it would "continue to monitor the implementation of both instrument. "

"Accession to the EU-US Privacy Shield program is entirely voluntary, but when an individual eligible entity publicly undertakes to meet the requirements of the system, the obligation becomes enforceable under US law."[24]

Court of Justice of the European Union No 91/20 Luxembourg, "On 16 June 2020, it issued a judgment declaring the decision of the European Commission (EU) 2016/1250 on the adequacy of data protection provided through the EU-US Privacy Shield invalid. The result of this decision is that the framework for harmonisation with the European legal regulations on personal data protection established by it no longer represents a valid mechanism of legal harmonisation in the transfer of personal data from the EU to the USA. Although the decision of the European Court of Justice is unequivocal, the official website of the Privacy Shield states that the US Department will continue to administer the program in terms of further processing submissions for self-certification and recertification of entities and maintain a list of those who have successfully certified. they shall send it to the European Commission, European national supervisory authorities or legal advisers for further information."[25] So, a new period of lively negotiations between the EU and the USA on the mentioned issue follows.

3.1. Data encryption and communication

"Encryption plays a key role in the digital space because it secures digital systems and transactions and protects a number of fundamental rights, including freedom of expression, privacy and data protection.

However, if it is used for the purpose of committing a criminal offence, it conceals the identity of criminals and the content of their communication."[26].

[24] The EU court declared the EU-US Privacy Shield invalid! Where is our personal data really? https://lidermedia.hr/sto-i-kako/sud-eu-a-proglasio-nevazecim-eu-us-stit-privatnosti-gdje-su-stvarno-nasi-osobni-podaci-132479

[25] The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[26] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, TO THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy for Combating Organized Crime for the Period 2021-2025 https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52021DC0170&from=EN

"In its 11th progress report on establishing an effective and genuine security union, the Commission proposed six practical measures to support law enforcement and judicial authorities when they encounter encrypted data stored on devices (such as telephones and hard drives) in criminal investigations. , without the need to prohibit, restrict or weaken encryption. These measures also include Europol's new decryption tool, launched by the Commission in December 2020, which will help address these issues. The European Cybercrime Training and Education Group (ECTEG), funded by the Internal Security Fund - Police, has developed training modules and conducted pilot courses. These courses will be included in the regular training offered at the European Police Academy (CEPOL)"[27], where police officers of the Ministry of the Interior of the Republic of Croatia should be actively involved to learn and practice the necessary knowledge and skills.

It would also be essential to design courses, thematic units and curricula with content from this domain and their inclusion in various forms of training at the Police Academy.

"The needs of investigators on the Internet must be reliably determined. Europol, in accordance with its powers, and the EU Security Innovation Center will coordinate a comprehensive analysis of technological gaps and needs in the field of digital investigations and analysis with predictions. Research and innovation are necessary both for the development of technologies for investigations and for the fight against crimes committed with the help of digital technology. CEPOL and the European Judicial Training Network (EJTN) will work closely with experts and Member States to develop certification/accreditation programs for digital investigators."[28]

Some countries have noticed some difficulties in encrypting communications and have decided to solve this problem with new legislation, so in early December 2018, the Australian Parliament adopted a new encryption law that will force technology companies to provide access to law enforcement and security agencies-encrypted communications.

The Australian Decryption Act allows state law enforcement agencies to force companies to hand over user data even though they are protected by cryptography; if companies do not have the power to intercept encrypted data for the authorities, they will be forced to create tools to give police or government access to their users' data.

This is a concept that many consider bad because they say: A home door for one is a back door for all. The disadvantage of this law is that the creation of tools for weakening cryptography for one purpose is weak for all functions. People around the world depend on cryptography for their security in many areas of life.

The tools that will have to be created to intercept encrypted messages between suspected terrorists could undermine the digital security of anyone doing business with Australia or United Nations member states.

[27] Ibid p. 25.

[28] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,TO THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy for Combating Organized Crime for the Period 2021-2025 https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170

People around the world depend on cryptography for their security in many areas of life, whether they buy things online, manage their current accounts, or use it for private personal or business communication.

The Coalition for Government Oversight Reform (RGS), which includes Microsoft, Apple, Facebook and others, has strongly opposed the law because it threatens the privacy and security of their users' data.

3.2. Private sector and security standards

Representatives of the private sector also play an unavoidable and important role in the overall activities regarding the interception and collection of data from the Internet and the cloud, as evidenced by the previous and the following example.

"Amazon Web Services (AWS) is the most comprehensive and widely accepted cloud platform in the world, offering over 200 fully equipped data centre services worldwide. Millions of customers - including the fastest growing startups, the largest companies and leading government agencies - use AWS to cut costs, become more agile and innovate faster."[29]

AWS's obligations go beyond what is required by the Schrems II judgment and are currently provided by other cloud service providers to protect the personal data that users entrust to AWS to process (user data). Significantly, these new obligations apply to all customer data subject to the GDPR processed by AWS, whether or not they are transferred outside the European Economic Area (EEA).

AWS enhanced contractual obligations include:

Challenging law enforcement requests will therefore challenge law enforcement requests for customer data from government bodies, either within or outside the EEA, where the request is in conflict with EU law, too extensive or if the AWS otherwise has any appropriate basis for that.

Disclosure of the minimum amount required, whereby AWS undertakes that, despite AWS standards, if ever compelled by a valid and binding legal requirement to disclose customer data, it will disclose only the minimum amount of customer data required to comply with the request.

These enhanced AWS obligations to customers build on AWS's long list of records of law enforcement requirements. AWS rigorously limits - or completely rejects - law enforcement requirements for data coming from any country, including the United States, that is too broad or AWS has any appropriate basis for doing so.

These commitments further demonstrate AWS's commitment to providing data to its customers, which is AWS' highest priority. AWS implements rigorous contractual, technical and organisational measures to protect the confidentiality, integrity and availability of user data, regardless of which AWS region the user chooses. AWS users have complete control over their data through powerful AWS services and tools that allow them to determine where the data will be stored, how it is protected and who can access it.

[29] Cloud computing with AWS https://aws.amazon.com/what-is-aws/

4. CONCLUSION

This work sought to support and inform decision-makers in taking clear national positions regarding these controversial legal norms and their mutual conflicts.

The Croatian Minister of Justice and Public Administration has signed the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, showing that its ratification is underway and that Croatia is on the right track in seeking common EU solutions.

The next important message is the initiative to design a course program that would deal with the study of the legal basis for collecting digital evidence from the Internet and the cloud at the undergraduate and graduate level of education, i.e. based on scientific research, creating the basis for the improvement of educational content at the Police Academy, at all levels of education and training, including lifelong learning.

Training courses in the field of collecting digital evidence from the Internet and the cloud are actively conducted at the European Police Academy (CEPOL), where police officers should also be actively involved in learning and practising the necessary knowledge and skills, primarily due to the need developing the interoperability capabilities needed for joint actions in combating crime of international dimensions.

The paper clearly identifies the need for procurement of adequate hardware and software for constructing and establishing a digital forensic laboratory for digital forensics of the Internet and clouds, and the design of SOPs for their application and targeted training and specialisation of participants selected from the lines of work, present in the performance of daily tasks.

REFERENCES

1. Cloud computing with AWS, https://aws.amazon.com/what-is-aws/
2. European Union Serious and Organised Crime Threat Assessment, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
3. EUROPEAN COMMISSION, Brussels, 14.4.2021, COM (2021) 170 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, on an EU Strategy to Combat Organised Crime 2021.–2025 https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52021DC0170&from=EN
4. EUROPEAN COMMISSION, Brussels, 25.11.2021, COM (2021) 719 final 2021/0383 (NLE), Proposal for a COUNCIL DECISION authorising the Member States to ratify, in the interests of the European Union, the Second Additional Protocol to the Convention on Cybercrime concerning Enhanced Co-operation and detection of electronic evidence, https://eur-lex.europa.eu/resource.html?uri=cellar:19142d38-4e22-11ec-91ac-01aa75ed71a1.0018.02/DOC_1&format=PDF

5. EUROPEAN COMMISSION, Strasbourg, 17.4.2018, COM (2018) 225 final, 2018/0108 (COD), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European order for delivery and the European order for the safekeeping of electronic evidence in criminal matters https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:52018PC0225&from=EN
6. COMMUNICATIONFROMTHECOMMISSIONTOTHEEUROPEANPARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy for the Suppression of Organized Crime for the period 2021.–2025., Document 52021DC0170, COM/2021/170 final, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A52021DC0170
7. Lider: EU court declares invalid EU-US Privacy Shield! Where is our personal information really? July 21, 2020. https://lidermedia.hr/sto-i-kako/sud-eu-a-proglasio-nevazecim-eu-us-stit-privatnosti-gdje-su-stvarno-nasi-osobni-podaci-132479
8. Mapping the risk of serious and organised crime infiltrating legitimate businesses https://data.europa.eu/doi/10.2837/64101
9. DECISION ON THE PROMULGATION OF THE LAW ON THE CONFIRMATION OF THE CONVENTION ON CYBERNETIC CRIME https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html
10. Plenković, M. i Mustić, D. (2020). Paradigmatic reflections on media, culture and public relations. *Informatologia, 53* (1-2), 53-91. https://doi.org/10.32914/i.53.1-2.5
11. Press and Information: Court of Justice of the European Union, PRESS RELEASE No 91/20, Luxembourg, 16 July 2020, Judgment in Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf
12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European order for service and the European order for the safeguarding of electronic evidence in criminal matters, https://data.consilium.europa.eu/doc/document/ST-8110-2018-INIT/hr/pdf
13. Strasbourg, April 17, 2018. SWD (2018) 119 final COMMISSION STAFF WORKING DOCUMENT SUMMARY OF THE IMPACT ASSESSMENT attached to the document Proposal for a Regulation of the European Parliament and of the Council on the European Delivery Order and the European Order for the Preservation of Electronic Evidence in Criminal Matters and Proposal for a Directive representatives for the purpose of gathering evidence in criminal proceedings {COM(2018) 225 final} - {COM(2018) 226 final} - {SWD(2018) 118 final} SWD(2018)119/F1 – HR
14. REGULATION, ON OBLIGATIONS IN THE FIELD OF NATIONAL SECURITY OF THE REPUBLIC OF CROATIA FOR LEGAL ENTITIES AND NATURAL PERSONS IN TELECOMMUNICATIONS https://narodne-novine.nn.hr/clanci/sluzbeni/2003_05_83_1013.html
15. EU Council, Press Release, 5 April 2022, 11:00, Access to e-evidence: Council authorises

Member States to sign international agreement https://www.consilium.europa.eu/hr/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/

Sažetak

Krunoslav Antoliš

Izazovi prekograničnog prikupljanja digitalnih dokaza

U suvremenom svijetu upotreba informacijsko-komunikacijskih tehnologija (IKT) postala je dio života. IKT infrastruktura nositelj je digitalnih tragova: legalnih i ilegalnih aktivnosti koje se putem nje obavljaju. No da bi nešto postalo digitalni dokaz, zakonom ovlaštena osoba to mora i zakonski pribaviti. Naime, virtualna infrastruktura, posebice internet i novi izazovi koje nam donosi arhitektura oblaka zbog česte fizičke pozicioniranosti izvan državnih granica, dovodi u pitanje zakonitost pretraživanja i prikupljanja digitalnih dokaza izvan državnih granica. Ovaj rad analizira pravnu osnovu za prikupljanje digitalnih dokaza u kibernetičkom prostoru na međunarodnoj razini, kao što su: Konvencija Vijeća Europe o kibernetičkom kriminalu, američki Cloud Act, australski Zakon o dešifriranju i europski GDPR. Iako je Sud Europske unije proglasio nevažećom odluku Europske komisije (EU) 2016/1250 o primjerenosti zaštite podataka kroz EU-US Privacy Shield, stručnjaci ne smiju prestati tražiti rješenje tog evidentnog problema. Rad ima namjeru podržati donositelje odluka u zauzimanju jasnih nacionalnih stavova o navedenim kontroverznim pravnim normama i njihovu međusobnom sukobu. U radu se uspoređuju pravne posljedice takvog prikupljanja i prihvatljivost takvog digitalnog dokaza, a takvo prikupljanje može biti povezano i s povredom privatnosti pravne i fizičke osobe.

Ključne riječi: *digitalni dokazi, prekogranični pristup, pravni standardi, internet, oblak.*