THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 16 Article 3

September 2021

The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities

Paweł Olber Dr
Police Academy in Szczytno, Poland, p.olber@wspol.edu.pl

The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities

Cover Page Footnote

This work is published as part of the research task: "Legal and technical aspects of securing digital data from cloud computing, task code: ISK-2/2018, financed from a subsidy by the Ministry of Interior and Administration, granted for maintaining and developing the research potential of the Police Academy in Szczytno, Poland.

THE SURVEY ON CROSS-BORDER COLLECTION OF DIGITAL EVIDENCE BY REPRESENTATIVES FROM POLISH PROSECUTORS' OFFICES AND JUDICIAL AUTHORITIES

Paweł Olber
Department of Forensics and Computer Forensics, Institute of Criminal Service
Police Academy in Szczytno
Marszałka Józefa Piłsudskiego 111, Szczytno, Poland
p.olber@wspol.edu.pl

ABSTRACT

Dynamic development of IT technology poses new challenges related to the cross-border collection of electronic evidence from the cloud. Many times investigators need to secure data stored on foreign servers directly and then look for solutions on how to turn the data into a legitimate source of evidence. To study the situation and propose solutions, I conducted a survey among Polish representatives of public prosecutors' offices and courts. This paper presents information from digital evidence collection practices across multiple jurisdictions. I stated that representatives from the prosecution and the judiciary in Poland are aware of the issues associated with cross-border acquisition and preservation of cloud-based evidence. In their view, many of the problems are time-consuming and ineffective international cooperation, the voluntary nature of cooperation between foreign cloud service providers, lack of harmonized procedures and guidelines, the diversity of legal systems, and the lack of knowledge held by law enforcement officials and the judiciary. This work should be the beginning of an open discussion with practitioners about existing challenges and an invitation for further research with a larger sample of prosecutors and judges. There are no such studies in literature. The paper shows that it is possible to improve current procedures for the cross-border collection of cloud-based digital evidence.

Keywords: digital evidence, computer forensics, digital investigation, international cooperation, cybercrime, cross-border investigation, jurisdiction, remote search.

1. INTRODUCTION

Several years ago, Brenner & Schwerha (2002) stated that the gathering of digital evidence across national borders would be a challenge for law enforcement and judicial authorities ahead. The authors did not strictly define the duration of this challenge, stating only that cross-border collection of digital evidence would be a problem for some time

(Brenner & Schwerha, 2002). Probably that academics were not aware of how important this problem would be ahead. Based on the current state of digital evidence collection, the statement by Brenner & Schwerha (2002) has become prophetic. Gathering digital evidence causes frustration among cybercrime detectives, prosecutors, and foreign affairs ministers (James & Gladyshev, 2016). The lack of a wide global legal framework for the collection of digital evidence encourages states to apply their own solutions. These activities focus on overcoming existing jurisdictional barriers and do not always comply with existing legal rules (Çela, 2015).The situation is like Polish police officers and representatives from prosecutors' offices and the judiciary.

My observations and experiences show that in their actions are a lack of sufficient knowledge concerning cloud computing technology, the technical possibilities of securing digital evidence in the cloud, and legal regulations in this area. Investigators secure data stored on foreign servers directly. The law does not permit access to such resources without international legal assistance. After acquired data, investigators seek solutions on how to turn the data into a legal source of evidence (Opitek, 2018).

The described problem is essential because law enforcement and justice should collect digital evidence quickly and under the law. However, this is a very complex issue because most times digital evidence is subject to multiple jurisdictions. Representatives of law enforcement and the judiciary avoid talking about the difficulties that exist, which makes it difficult to solve the problem. The survey enabled the collection of information from representatives of prosecutors and courts about their practice, a key element of this study.

1.1 Contribution

This work contributes importantly to the area of law and computer forensics, the purpose to provide digital evidence of crimes committed. Specifically, this work provides information relating to practices applied in acquiring and preserving digital evidence by Polish prosecutors and the judiciary. Moreover, it points out the changes in this area. The problem of cross-border digital evidence collection is worldwide (Cole & Quintel, 2018). This work should be the beginning of an open discussion about existing challenges. Based on the results of the research, representatives of the prosecutor's office should know that deputing the police to secure data from foreign servers as part of technical activities is unacceptable.

The results of the study should change the current practice, which comprises ordering the police to secure data from foreign servers. Prosecutors should realize that collecting digital evidence requires using legal instruments. To this, it is also important to take advantage of a 24/7 contact point. Readers can use research results for train law enforcement agencies and judicial authorities.

1.2 The current state of affairs

On the European level, it deals with these issues of the Council of Europe and the European Union. These institutions were the first to act to adapt existing legislation to a changing world (Karatysz, 2014). These bodies address issues related to cross-border access to digital evidence and ways of securing it. The Council of Europe, which had already adopted the Convention on Cybercrime (CETS No.185) in 2001, completed most of the work. This institution established the Cybercrime Convention Committee (T-CY) ("Details of Treaty No. 185 Convention on Cybercrime," n.d.). The major task of the T-CY Committee is to collect info on the current legal situation in countries, propose

projects, conduct studies and publish reports. T-CY Committee prepared two reports on mutual legal assistance (T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 2014, Transborder access to data and jurisdiction: Options for further action by the T-CY, 2014). These documents have options for better proceeding on cross-border access to digital evidence and jurisdiction. These papers involve suggestions addressed to the Parties of the Cybercrime Convention, to increase international legal cooperation and cross-border acquisition of electronic evidence, and also address jurisdiction.

1.3 Literature review

The literature review shows that the TC-Y Committee conducted a study on the actions taken by the Parties to improve the cross-border acquisition of digital evidence and focused on multi-jurisdictional legal assistance organizations. The research involved 40 States Parties to the Convention and 1 Observer State (Follow up to the Assessment Report on Mutual Legal Assistance–T-CY(2013)17revCompilation of replies to the questionnaire, 2017). Jõgi, Kaldoja, Luuk & Randma (2018) analyze these studies, stressing that no single common approach for the cross-border collection of digital evidence. States are developing their own internal solutions. James & Gladyshev (2016) conducted similar studies only on mutual legal assistance. Osula & Zoetekouw (2017) compare distinct notification requirements for remote search and seizure only in three countries.

Previous research showed not any comprehensive scientific study with the results of a diagnostic survey on cross-border collecting of digital evidence with various legal instruments and other solutions, based on the skill and practice of law enforcement and the judiciary.

Recent studies have shown that cross-border digital evidence gathering is relating to cloud computing. Carthy, Crosbie, Kechadi & Ruan (2011) define this term as a paradigm with complex aspects. The complexity of the cloud is because of its structure, which comprises many resources: networks, servers, storage, applications and services. Data centers are also located all over the world. This means that data replication takes place in many locations and in distinct jurisdictions. All these make cloud computing a problem for law enforcement and the judiciary and hamper the collection of digital evidence. Hurst et al. (2014) list 65 major forensic challenges which include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards and training. Scientists studied these areas over the past years. However, many challenges remain unresolved. I present the results of the research conducted so far related to the problem of collecting electronic evidence from clouds in the following paragraphs.

Dharaskar, Patil & Thakare (2017) identify the lack of a specific framework for computer forensics at distinct levels of cloud computing services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This is also what Erlin, Lizarti & Sudyana (2019) point out when investigating a server in the private cloud. The situation is further complicated by private enterprise clouds (Wang & Wang, 2012). The case is even more problematic for public cloud computing services where CSP plays a leading role. Service providers have control over the data and all the information. Investigators depend on CSPs if they need digital evidence, including network and server logs (Ali, Memon, Sahito, 2018). It is therefore essential to develop cloud-based forensic tools and solutions that will reduce depen-

dence on CSP (Choo, Conti, Gaur, Manral & Somani, 2020).

To minimize the difficulties with collecting digital evidence from the clouds, many researchers pay attention to the possibilities offered by traditional computer forensics. Dargahi & Dehghantanha (2017) discovered that the local device contains forensic data relating to CloudMe and 360Yunpan accounts. The authors show that user credentials, device names, filenames, and evidence of activity are on hard drives, in volatile memory, and backup files. Data are also in the memory of mobile devices (Horng, Huang, Ko, Wang & Zhuang, 2021). Investigating an iOS device, the authors revealed artifacts related to OneDrive, Dropbox and Google Drive.

According to Horsman (2020), data related to cloud services read from the memory of devices can justify a request sent to a CSP. By analyzing the devices connected to the cloud, investigators can collect user data and information about files stored in the cloud (Ahmad, Ariffin, Hamid & Shahidan, 2020). Web browsers save many artifacts. By examining the suspect's hard drive and the contents of RAM, investigators can get potential digital evidence (Carpenter, Hill, Montasari & Montaseri, 2019). Such possibilities exist even with encrypted communication (Choo, Dehghantanha & Teing, 2018). The authors examined the CloudMe application and recovered the root directory of the web application from the web browser cache. Choo, Dehghantanha, & Mohtasebi (2017) investigated SpiderOak, JustCloud and pCloud services. They recovered e-mail addresses, the ID and name of the account, and the names of uploaded and downloaded files.

The second group of solutions uses various models and procedures. It's also relating to CSPs. According to Gritzalis, Kalloniatis, Katos & Simou (2019), cloud services should consider specific forensic requirements. This will allow for gathering evidence according to forensic principles. Another idea is to minimize law enforcement dependency on CSPs. Alex & Kishore (2017) proposed a centralized forensic server with a layer called the Forensic Monitoring Plane (FMP). Trenwith & Venter (2019) proposed a system for managing access to cloud facilities. Their solution uses the location of objects and an access control mechanism called the digital passport (FReadyPass). Other than the technical issues, the authors emphasize the complexity of legislative and jurisdictional issues.

The analysis of research shows that the key problem in collecting digital evidence from the clouds is a legal issue. Many experts highlight the challenges of multiple jurisdictions (Mohiddin, Sharmila & Yalavarthi, 2017). It's difficult to coordinate multiple jurisdictions (Ghosh & Majumder, 2021). This affects the investigation and delay in data access (Arora, Sakthivel & Sharma, 2018). Multiple jurisdictions means many laws, regulations, and agreements. This complexity means that sometimes a digital investigation ends up violating local law (Albakri et al., 2018). According to Conti, Dargahi & Dehghantanha (2017), the analysis of legal implications related to conducting forensic analysis in the could increase the possibilities of using cloud investigation techniques. Brown (2015) argues, however, that governments around the world show a reluctance to analyze the effectiveness of mechanisms for investigating serious cases of cybercrime.

Perhaps the solution should be to implement a universal law that would apply and would be subject to only one jurisdiction (Ajayi, 2016). However, the mere existence of legislation is not sufficient. Close regional and global cooperation is essential, also with internet service providers (Bërdufi & Dushi, 2017). The authors point out that, apart from jurisdictional issues, the awareness and knowledge of law enforcement authorities is also important. Based on his research, he con-

cludes that most law enforcement agencies do not have the technical knowledge, while internet criminals are experts in computer technology. One strategy to combat these crimes is to educate and develop human resources.

Mohammed & Mohammed, (2019) state that it is a widespread agreement among practitioners and researchers that cybercrime investigation hampers by insufficient knowledge and skills gaps in law enforcement and judiciary. The authors argue that as the amount and importance of digital evidence increases, judges must fairly assess them. They must have a general comprehension of the technologies. According to the authors, it's necessary to build awareness among lawmakers and law enforcement officers. Mahanamahewa & Perera (2017) shows that the lack of adequate support and regulations make it difficult for digital forensics experts to prepare and present acceptable evidence to the courts. This situation leads to delays in resolving cases.

According to Seger (2013), the efficient response of criminal justice is essential. Capacity building is fundamental as an approach to cybercrime. Elements of capacity building programs may include support for legislation, training, and cooperation. These programs should aim to increase the power of law enforcement. The tangible effects of this approach will improve the use of electronic evidence in criminal proceedings. Karie & Karume (2017) pointed out that many law enforcement agencies around the world are introducing proactive measures to increase their ability to respond to security incidents. They also create an environment known as digital forensic readiness.

Digital forensic readiness also produces many challenges. One of them is the lack of qualified digital forensics personnel. Staff training and compliance with a forensic readiness plan, however, can be an efficient measure. All staff members in the organization will know the correct procedures during the digital investigation process. Previous studies have almost only focused on digital forensic, models, jurisdiction, and building forensic competence and readiness. However, the source of data in these studies was not the knowledge and experience of representatives of law enforcement agencies and the judiciary. The only exception is Barrett's study (2017). She determined the possibilities to apply traditional forensic evidence gathering processes in cloud computing.

A scientist conducted a more recent study. Barrett (2020) got the judge of 14 experts on evidence gathering in the cloud environment and suggestions on how to prepare students for technological changes in data acquisition processes in the digital environment. Despite these studies, the problem of cross-border collection of digital evidence remains open. Therefore, the research question asked in this paper is stated as follows: What are the problems and difficulties faced by police officers, prosecutors, and the judiciary regarding actions taken to acquire and secure digital evidence from the cloud? This issue needs clarification by asking the more detailed questions:

- Is it possible to improve the current procedures for cross-border evidence collection from cloud computing, and what actions should be taken?
- Do police officers, prosecutors, and the judiciary have adequate knowledge about legal regulations concerning the access to digital evidence from the cloud?
- Why do police officers, prosecutors, and the judiciary use different legal bases regarding digital evidence collection?
- How do police officers, prosecutors, and the judiciary evaluate cooperate with foreign cloud service providers?

- What does the cooperation with the 24/7 contact point established by the Cybercrime Convention look like?

2. SURVEY CONSTRUCTION, VALIDATION AND PRETESTING

To get answers to the above questions, I organized a survey. Before the survey, I conducted a detailed literary analysis of the acquisition and preservation of digital evidence. The questionnaire contains 25 questions divided into the following four categories:

Practical-related questions: In this set of questions, the respondents provided information about their experience in secure electronic evidence in the cloud (Q1), used methods of proceeding (Q2), identified of problems (Q3), other known problems (Q4) and proposed solutions to the identified difficulties (Q5). I present the results in Appendix 1.

Cloud Service Provider-related questions: In this set of questions, the respondents were required to give information about their experience in cooperation with foreign cloud service providers (Q6), used regulations to send data access requests (Q7), opinion about needs improvement in this cooperation (Q8), known problems (Q9) and proposed solutions to the identified problems (Q10). I present the results in Appendix 2.

24/7 contact point-related questions: In this set of questions, the respondents provided information about their experience in cooperation with a 24/7 contact point (Q11), the scope of cooperation (Q12), elements that need to improvement (Q13), known problems (14) and proposed solutions to the identified difficulties (Q15). I present the results in Appendix 3.

Opinion and knowledge-related questions: In this set of questions, the respondents provided information about their knowledge of international activities to improve the procedures for acquiring digital evidence from the clouds (Q16, Q17), participation in training on cloud computing or cross-border collection of digital evidence (Q18-Q20) and knowledge of legislation (Q21 – Q25). I present the results in Appendix 4.

To test the reliability and accuracy of the questionnaire, I conducted a pilot study among 40 court representatives who took part in the cybercrime training in Police Academy in Szczytno, Poland (`https://www.kssip.gov.pl/node/5805`). After collecting the questionnaires, I discussed all comments and observations with the participants. Then I checked the answers and additional comments. This approach allowed for the final refinement of the questionnaire by making the selected questions more detailed. After this piloting process, the questionnaire was ready for the larger audience. The questionnaire is available at (Olber, 2019).

2.1 Population and sampling

The criterion for selecting the sample for the research was professional affiliation, and the activities performed. Because of the specific nature of the research issues, I assumed the target group would be computer forensic experts from Polish police forensic laboratories and specialists from the Bureau/Departments for Combating Cybercrime, as well as representatives from prosecutors' offices and the judiciary. However, I did not receive permission to conduct opinion polls within the police. I conducted research in the end of 2018 exclusively among representatives from Polish prosecutors' offices and the judiciary. The survey involved 142 respondents. However, I distributed the questionnaires to 243 people. One theory to explain the low number of responses may be respondents' desire to avoid admitting to insufficient knowledge

of digital evidence regarding its acquisition and preservation.

2.2 Data collection

I conducted the survey in November 2018. I distributed the survey to participants of trainings organized by the National School of Judiciary and Public Prosecution in Cracow, Poland (`https://www.kssip.gov.pl/angielski`).

2.3 Data validation and analysis

I checked all the surveys received for completeness. I found that, among the collected questionnaires, 3 had missing data in closed questions and discarded them. One questionnaire did not include a sign of gender (metric). Here, the sum of observations is 138 and in the other questions 139.

2.4 Statistical tests

I conducted a statistical analysis of the survey results using IBM SPSS Statistics. I recorded the results of the survey as cross-tabulations. Then, I compared the responses of the prosecution and court employees and checked all the correlations. I categorized the responses for the open-ended questions. I analyzed the categories similar to the closed questions. In the analysis, I used the following test and statistical coefficient to examine the relationships: I used the Chi-square test to see the relationship between nominal variables or between nominal and ordinal variables. N values determine the size of the study set.

For all statistical tests, the level of significance was set to P = 0.05. I used Cramer's V coefficient to test how strong the correlation is between the nominal variables or between the nominal, ordinal variable. I calculated Cramer's V statistic when the Chi-square test produced a significant result, under the condition of group independence and the number of expected observations. This value can range from 0 to 1. The higher the value, the stronger the correlation between the variables. In the study, I adopted the numerical intervals: |0,0 – 0,2| – very weak relationship; |0,2 – 0,4| – weak relationship; |0,4 – 0,6| – moderate dependence; |0,6 – 0,8| – strong dependence; |0,8 – 1,0| – very strong dependence.

3. RESULTS

This section summarizes the survey results and starts by presenting the characteristics of the respondents.

3.1 Demographics

Two groups of respondents took part in the study, prosecution representatives N = 57 and judicial representatives N = 81. More than half of the surveyed representatives from prosecutors' offices (64.9%, N = 37) and representatives from the courts (64.2%, N = 89) are women. Men were the other 35.1%, N = 20 of the surveyed representatives from prosecutors' offices and 35.8%, N = 29 of the surveyed court employees. I present the results of demographics in Table 1.

3.2 General questions

This section addresses questions according to the division presented in section Survey construction. The following questions will allow to identify the level of knowledge and awareness and the prosecution and judiciary's standard practices relating to the cross-border collection of digital evidence, including from cloud-based services.

3.2.1 Practical-related questions

The research shows that only one in four prosecutorial employees, and so 24.1%, N = 14 and only 3.7%, N = 3 of court staff faced the need to secure cross-border digital evidence in the cloud. Prosecutorial respondents most

Table 1. Group of respondents

Gender	Prosecutors' offices		Court		Total	
	N	%	N	%	N	%
Woman	*37*	*64.9%*	*52*	*64.2%*	*89*	*64.5%*
Man	*20*	*35.1%*	*29*	*35.8%*	*49*	*35.5%*
Total	*57*	*100.0%*	*81*	*100.0%*	*138*	*100.0%*
Test: Chi-square=0.007, p=0.931, Cramer's V=0.007						

often pointed to a legal decision to request data and search of an IT system – 4.9%, N = 4. The other answers given by the prosecution were: the use of mutual legal assistance (2.5%, N = 2), appointing an IT expert (1.2%, N = 1), and get a username and password and the self-directed login to the resources (1.2%, N = 1). Court representatives (individuals), pointed to the legal decision to request data, the appointment of an expert, and the order for expert examination. The research shows that many more prosecutorial employees (48.3%, N = 28) than court employees (28.4%, N = 51) believe that getting digital evidence from foreign cloud servers is a problem for law enforcement authorities. In contrast, far more court employees (66.7%, N = 79) than prosecutorial employees (43.1%, N = 54) have no knowledge or opinion about the subject. According to the respondents, the problems in preserving and acquiring digital evidence are: - ineffective international cooperation, and the voluntary nature of cooperation with foreign service providers (11.5% each, N = 16); - lack of standard procedures and guidelines (98.6%, N=12); - diversity of legal systems, lack of knowledge, location of servers outside the country, location of cloud service providers outside the country, lack of software and technical solutions, distinct data retention time, anti-forensic solutions, and identification of the offender (mentioned by maximum 6 people). Prosecutorial employees most often see the problem of the voluntary nature of cooperation with foreign cloud service providers (15.5%, N = 9), and court employees most frequently see the problem of time-consuming and ineffective international cooperation (11.1%, N = 9). Regarding the problems presented by the respondents, it is important to pay attention to the solutions proposed by them. Respondents most often pointed to develop effective legal regulations (7.2%, N = 10), and less often to the train of law enforcement and judicial authorities (5%, N = 7), improvement of international cooperation (3.6%, N = 5) and development of procedures and guidelines (3.6%, N = 5). Maximum 2 persons choose the remaining methods, such as increasing the financial budget, the obligation for foreign cloud service providers to cooperate, and unification of legal systems. It is interesting to note that only prosecutors' staff (8.6%, N = 5) proposed improving international cooperation.

3.2.2 Cloud Service Provider-related questions

The research shows that many more prosecutorial employees (29.3%, N = 17) than court employees (7.4%, N = 6) have applied to a foreign cloud service provider to acquire digital evidence. To send data access requests to foreign cloud service providers responders most often used Mutual Legal Assistance (7.9%, N = 11) and less frequently to the

European Investigation Order (5.8%, N = 8). The answers also included national legislation (3.6%, N = 5), informal cooperation (2.2%, N = 3) and the Cybercrime Convention (0.7%, N = 1). Many more prosecutorial employees (37.9%, N = 22) than court employees (18.5%, N = 15) believe that cooperation between Polish procedural authorities and foreign cloud service providers needs improvement. The similar percentage of prosecutorial employees (5.2%, N = 3) and court employees (4.9%, N = 4) have a different opinion. The respondents questioned about specific problems regarding cooperation with foreign cloud service providers most pointed to the time-consuming nature of cooperation (10.1%, N = 14), and less to the voluntary nature of cooperation with foreign cloud service providers (5.8%, N = 8) and the lack of regulations concerning direct cooperation with such providers (5.8%, N = 8). Maximum 3 respondents each mentioned the other problems, such as the diversity of legal systems, language differences, diversity of data retention time, ignorance of foreign legal regulations, and lack of standard procedures and guidelines.

Respondents queried about proposed solutions to problems related to the Polish authorities' cooperation with foreign cloud service providers most often pointed to (3.6% each, N = 5) the obligation on foreign cloud service providers to respond, develop effective legal regulations and use the assistance of a 24/7 contact point, and slightly less (2.9%, N = 4) to improve international cooperation. Maximum 2 people gave the remaining answers, such as effective use of existing legal instruments, training of law enforcement authorities and the judiciary, unification of data requests, and unification of data retention time.

3.2.3 24/7 contact point-related questions

Only a few prosecutorial staff (8.6%, N = 5) and court staff (1.2%, N = 1) cooperated with the 24/7 contact point. This cooperation involved primarily technical consulting (2.9%, N = 4). Prosecutorial employees (8.9%, N = 5) and court employees (3.7%, N = 3) believe that needs to improve this cooperation. Many court employees (92.6%, N = 75) and prosecutorial employees (82.1%, N = 82.1) had no opinion (and/or knowledge) on this subject. Respondents queried about aspects requiring improved pointed to the need of dissemination of information on the principles of cooperation (2.9%, N = 4) and need to prepare training courses (0.7% – only one person). The same responders proposed solutions and pointed, that it is necessary to disseminate information on the principles of cooperation and ongoing exchange of information with the 24/7 contact point.

3.2.4 Opinion and knowledge-related questions

Only a few respondents, namely 3.4%, N = 2 from the prosecution and 1.3%, N = 1 from courts are familiar with international activities related to the improvement of procedures for obtaining digital evidence in the cloud. They listed initiatives: the build of a platform for exchanging the European Investigation Order in electronic form (one prosecutor) and the European Investigation Order (one court employee). The survey participants were not aware of this. I should note that none of the respondents mentioned the work carried out by the Council of Europe, in particular the TC-Y Committee and the Cloud Evidence Group, which are important for cross-border gathering of digital evidence. More respondents working in prosecutors' offices (10.3%, N = 6) than in the court (3.7%, N = 3) took part in training covering the issues of cross-

border acquisition of digital evidence. Most of them took part in training in preventing and combating cybercrime (5%, N = 7).

More court employees (33.3%, N = 27) than prosecutorial employees (22.4%, N = 13) wrongly believe that the Polish police have procedural rights to remotely search IT resources and acquire digital evidence in this manner. Contrary opinions (which are correct) expressed by far more prosecutorial staff (19%, N = 11) than by court staff (3.7%, N = 3). More prosecutorial employees (51.7%, N = 30) than court employees (32.1%, N = 26) believe that it is legal to search the content of an e-mail inbox, available via a web browser operated by a foreign operator. Less than 10% of the respondents gave (in the author's opinion) the correct answer. Many more court staff (58%, N = 47) than prosecutors (41.4%, N = 24) do not have this knowledge. According to the respondents, the search of e-mail sources should do with visual examination (32.4%, N = 45), and less (22.2%, N = 31) by the search of an IT system.

Fewer respondents chose the remaining answers, forensic expertise (6.5%, N = 9), procedural control (2.2%, N = 3), and experimental reconstruction (0.7%, N = 1). Asked which element most determines the legality of getting digital cloud-based evidence, the respondents most pointed to the crime scene (28.8%, N = 40). Nearly the same (28.1%, N = 39) admitted to a lack of knowledge. Many believed it is the location of the headquarters of the service provider (15.8%, N = 22) or the location of stored data (13.7%, N = 19). The other answers were: the location of the person who owns or controls the data (9.4%, N = 13), the location of the offender (8.6%, N = 12), the location of the service provider (6.5%, N = 9), the location of the victim (6.5%, N = 9), and the location of the service provider's representative (5.0%, N = 7).

Analyzing the answers, we should note that with serious crimes, we may consider two options: the crime scene and the place where the effect of the offense. Responders asked about a basis for remote searches or other means of acquiring data located outside the country most often admitted to lack of knowledge (45.3%, N = 63). The two most frequently pointed out concrete answers were: when data are publicly available and makes up an open-source of information (22.3%, N = 31) and after obtaining the consent of a person allowed to disclose IT data (19.4%, N = 27) – both correct. Many wrongly believed that a remote search or other methods of remote access to data outside the country is possible where the search concerns a service provider operating in a country that has ratified the Cybercrime Convention (CETS) (15.8%, N = 22), inability to identify a service provider (10.8%, N = 15) and the procedural control (10.1%, N = 14). The smallest number of respondents indicated a lack of knowledge about data location (5.8%, N = 8) and a lack of certainty about data location (5.8%, N = 8).

3.2.5 Statistical coefficient

As a result of the statistical analysis, I found significant relationships between variables in the following survey questions: Q1 - Q6, Q8, Q9, Q11, Q21, Q24. The obtained values of the significance level limits for these questions, lead me to accept the hypotheses: - Prosecutors had a stronger need to secure cloud-based digital evidence than the judiciary. - When it is necessary to secure evidence in the cloud, only prosecutors use a search of the computer system. - Prosecutorial employees are much more convinced that getting digital evidence from cloud computing is a problem. - More prosecutorial employees than of the courts perceive a problem with the diversity of legal systems. - Only prosecution staff believe that the so-

lution to cloud evidence collecting problems lies in improving international cooperation. - Significantly more prosecutors submitted an application to get electronic evidence from a foreign cloud service provider than court representatives. - Prosecutorial employees are much more likely than court employees that cooperation between law enforcement authorities and service providers needs to improve. - Significantly more prosecutorial employees than of the courts note the problem of the lack of procedural regulations regarding direct cooperation with foreign service providers. - More employees of the prosecutorial employees than of the courts worked with a 24/7 point of contact. - Significantly more employees of the prosecutorial employees than of the courts have a good knowledge of procedural rights regarding remote searches of IT resources. - Representatives of prosecutors and courts have no knowledge or opinion about the competence of national law enforcement and justice agencies to get electronic evidence from clouds. I should emphasize that the statistical significance found is not the same as the actual significance. The above statements should be interpreted as a basis for further consideration and inquiry.

3.2.6 Summary of the survey

This section summarizes the survey findings.

1. Representatives from public prosecutors' offices and the judiciary in Poland are aware of problems related to the cross-border collection of digital cloud-based evidence. However, they are not sure about the correct approach and the legal basis.

2. The problem in digital cloud-based evidence acquisition is the lack of service providers' willingness to cooperate. The deficit of adequate equipment for national law enforcement authorities with tools enabling to acquire digital evidence. Lack of knowledge in international cooperation and cloud computing technology.

3. Polish representatives from the prosecution and the judiciary do not fully use the potential of the 24/7 contact point for international cooperation and collect digital evidence. The 24/7 contact point does not promote its own role among national authorities.

4. Representatives of the prosecution and the judiciary in Poland do not have a uniform approach to collecting of digital evidence from clouds. They secure digital evidence as part of various procedural activities (examination, a search of an IT system, procedural experiment).

5. It is possible to improve current procedures for the cross-border collection of cloud-based digital evidence. It requires full using existing legal instruments, using the 24/7 contact point, providing training in international cooperation and cloud computing, and developing and implementing mechanisms to monitor the effectiveness of the international partnership.

4. WEAKNESSES

During the analysis of the problem of cross-border collecting of cloud-based digital evidence, I encountered difficulties because of the lack of literature on this topic. It led to analyzing existing legal regulations and reports from the Council of Europe and the European Union. Another problem included developing questionnaires of one type for various groups of respondents: representatives from courts and prosecutors' offices, and police computer forensic experts and specialists in cybercrime, although the police did not take part in the study. The following limitation was the lengthy procedure for obtaining

permission to conduct research among police officers, which was unsuccessful because of a lack of consent from senior police officials. The other limitation was that some participants did not complete the questionnaires. This may have resulted from a desire to avoid admitting to insufficient knowledge of digital evidence regarding its acquisition and preservation.

5. CONCLUSIONS

The paper concludes by arguing that representatives from the prosecution and the judiciary in Poland are aware of the issues associated with cross-border acquisition and preservation of cloud-based evidence. According to the respondents, the main problems are time-consuming and ineffective international cooperation, the voluntary nature of cooperation between foreign cloud service providers, lack of harmonized procedures and guidelines, the diversity of legal systems, and the lack of knowledge held by law enforcement officials and the judiciary.

Representatives from the prosecution and judiciary in Poland do not have sufficient knowledge (which, according to the respondents, is also a problem) about legal provisions regulating the cross-border acquisition of digital evidence. The respondents show that lack of knowledge in international cooperation and cloud computing technology is a major issue. Knowledge of the solutions and possibilities for digital evidence collection, and cloud computing technology itself, is essential. It is important to understand that the clouds use a virtualization mechanism and different models of services with specific features. Foreign entities with data centers located around the world offer these services. This raises many concerns about the possibility of independent access to resources by law enforcement representatives.

Lack of knowledge of the proper methods of proceeding and the legal basis of digital evidence acquisition causes Polish representatives from prosecutors' offices and the judiciary to commission the police to secure data on foreign servers. The police carry these tasks out within the framework of various process activities, most often the search of an IT system. However, legal regulations do not allow for the direct exploration of such data. Most representatives from prosecutors' offices and courts in Poland are not aware of the circumstances that may justify a remote search or other ways of obtaining remote access to data stored beyond national borders. This lack of awareness is because of unfamiliarity with the Cybercrime Convention. The Convention provides two possibilities to access digital data without the consent of the other country: publicly available data, and getting legally effective, voluntary consent from the person allowed to disclose such data.

A significant number of representatives from the prosecution and judiciary believe the Polish police have procedural powers in remote search of IT resources and the acquisition of digital evidence. However, Polish legislators have never passed laws enabling remote search of IT systems. Police officers should not conduct such activities. It is also wrong to believe that searching the contents of an e-mail inbox, owned by a foreign operator, complies with applicable legal regulations. Issues in cross-border acquisition of digital evidence from clouds results from uncertain cooperation with service providers, which is often lengthy and ineffective. The voluntary, variable and unreliable nature of this cooperation is also a problem. The service provider has a final decision on the disclosure of the data.

Polish law does not regulate direct cooperation between law enforcement authorities and foreign cloud service providers. There is also a lack of legal tools obligating foreign

cloud service providers to transfer data in the framework of foreign direct cooperation. Representatives from the Polish judiciary and prosecutors' offices do not use the full potential of the 24/7 contact point established by the Cybercrime Bureau of the Police National Police Headquarters. The 24/7 contact point does not promote itself among national authorities. There is the potential to take action at national and international levels to improve current procedures by which to acquire electronic cloud-based evidence.

5.1 Future work

Future research should aim to replicate the results on a larger sample of prosecutors and the judiciary. There is also a need to conduct a survey among police computer forensic experts and specialists in cybercrime. This will identify the genuine issues involved in collecting digital evidence subject to foreign jurisdiction.

REFERENCES

[1] Ahmad, N. H., Ariffin, K. A. Z., Hamid, A. S. S. A., & Shahidan, N. S. S. (2020). Cloud Forensic Analysis on pCloud: From Volatile Memory Perspectives. In M. Ali, M. P. S. Excell, H. Miraz, S. Soomro, & A. Ware (Eds.), Emerging Technologies in Computing. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, London, UK, August 19–20 (pp. 3-15). Cham: Springer.

[2] Ajayi, E. F. G. (2016). Challenges to Enforcement of Cyber-Crimes Laws and Policy. Journal of Internet and Information Systems, 6(1), 1-12. doi:10.5897/JIIS2015.0089 Albakri, S. H., Maarop, N., Magalingam, P., Perumal, S., Samy, G. N.,& Shanmugam, B. (2017). Digital forensic challenges in the cloud computing environment. In N. Gazem, F. Mohammed,

[3] S. Patnaik, F. Saeed, & A. S. Saed Balaid (Eds.), Recent Trends in Information and Communication Technology: Proceedings of the 2nd International Conference of Reliable Information and Communication Technology (IRICT 2017). Lecture Notes on Data Engineering and Communications Technologies, Johor Bahru, Malaysia, 23–24 April (669–676). Cham: Springer.

[4] Alex, M. E., Kishore R. (2017). Forensics Framework for Cloud Computing. Computers & Electrical Engineering, 60, 193-205. doi:10.1016/j.compeleceng.2017.02.006

[5] Ali, S. A., Memon, S. & Sahito F. (2018). Challenges and Solutions in Cloud Forensics. In Proceedings of the 2nd International Conference on Cloud and Big Data Computing - ICCBDC'18. Paper presented at 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018) and its workshop 2018 the 7th International Conference on Intelligent Information Processing (ICIIP 2018), Barcelona, Spain, 3-5 August (pp. 6–10). New York: ACM Press.

[6] Arora, D., Sakthivel, T., & Sharma, P. (2017). Mobile cloud forensic: Legal implications and counter measures. In A. Joshi & S. Satapathy (Eds.), Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1. Features the proceedings of ICTIS 2017: Second International Conference on Information and Communication Technology for Intelligent Systems, Ahmedabad, India, 25–26 March (pp. 531–542). Cham: Springer.

[7] Barrett, D. (2017). Applying a Contingency Framework to Digital Forensic Processes in Cloud Based Acquisitions. The Journal of Digital Forensics, Security and Law, 12(2), 75-96, doi:10.15394/jdfsl.2017.1473 Barrett, D. (2020). Cloud Based Evidence Acquisitions in Digital Forensic Education. Information Systems Education Journal, 18(6), 46-56.

[8] Bërdufi, N., & Dushi, D. (2017). Law Enforcement and Investigation of Cybercrime in Albania. European Scientific Journal, ESJ, 13(12), 575-592. Brenner, S. W., Schwerha IV, J. J. (2002), Transnational Evidence Gathering and Local Prosecution of International Cybercrime, Journal of Computer & Information Law, 20(3), 347-396.

[9] Brown, C. S. D. (2015). Investigating And Prosecuting Cyber Crime: Forensic Dependencies And Barriers To Justice. International Journal of Cyber Criminology, 9(1), 55-119. doi:10.5281/ZENODO.22387

[10] Carpenter, V., Hill, R., Montasari, R., & Montaseri, F. (2019). Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence. International Journal of Strategic Engineering, 2(1),52-60. doi:10.4018/IJoSE.2019010105

[11] Carthy J., Crosbie M., Kechadi T., & Ruan K. (2011) Cloud Forensics. In: G. Peterson & S. Shenoi (Eds.), Advances in Digital Forensics VII. 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, 31 January-2 February (pp. 35-46). Berlin: Springer.

[12] Çela, E. (2015) Situation in Astafur & Braanos in the case of legal representative for victimes, International Criminal Court (ICC) Moot Competition. Retrieved on June 20, 2020 from `https://www.academia.edu/12293178/cyber\_attacks\_case`.

[13] Choo, K. K. R., Conti, M., Gaur, M. S., Manral, B., & Somani, G. (2019). A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR), 52(6), 1-38. doi:10.1145/3361216

[14] Choo, K. K. R., Dehghantanha, A., & Mohtasebi, S. H. (2017). Cloud storage forensics: analysis of data remnants on SpiderOak, JustCloud, and pCloud. In K. K. R. Choo & A. Dehghantanha (Eds.), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, (pp. 205-246). Cambridge, United States: Elsevier.

[15] Choo, K. K. R., Dehghantanha, A., & Teing, Y. Y. (2018). CloudMe forensics: A case of big data forensic investigation. Concurrency and Computation: Practice and Experience, 30(5), 1-11. doi:10.1002/cpe.4277 Cole, M. D., Quintel, T. (2018). Transborder Access to e-Evidence by Law Enforcement Agencies, University of Luxembourg Law Working Paper, 10, 1-20, `http://dx.doi.org/10.2139/ssrn.3278780`.

[16] Conti, M. Dargahi, T., & Dehghantanha, A. (2017). Investigating Storage as a Service Cloud Platform: PCloud as a Case Study. In K. R. Choo & A. Dehghantanha (Eds.), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 185-204). Cambridge, United States: Elsevier.

[17] Council of Europe. (2009). The Cybercrime Convention Committee (T-CY).

T-CY (2009) 02 INF. Retrieved on June 24, 2020 from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Information_do_T-CY__2009_02-INF.pdf via the website: https://web.archive.org.

[18] Cybercrime Convention Committee (T-CY). (2017). Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers, T-CY(2017)2. Retrieved on July 2, 2020 from https://rm.coe.int/t-cy-2017-2-mla-follow-up-rep/168076d55f

[19] Cybercrime Convention Committee. (2014). Transborder access to data and jurisdiction: Options for further action by the T-CY, T-CY(2014)16. Retrieved on June 24, 2020 from https://rm.coe.int/cybercrime-convention-committee-t-cy-transborder-access-to-data-andju/168073dc0b.

[20] Dargahi, T., & Dehghantanha, A. (2017). Residual Cloud Forensics: CloudMe and 360Yunpan as case studies. In K. K. R. Choo & A. Dehghantanha (Eds.), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, (pp. 247-283). Cambridge, United States: Elsevier.

[21] De, D., Ghosh, A., & Majumder, K (2021). A Systematic Review of Digital, Cloud and IoT Forensics. In M. Chakraborty, M. Singh, V. E. Balas & I. Mukhopadhyay (Eds.), The "Essence" of Network Security: An End-to-End Panorama (pp. 31-74). Singapore: Springer Singapore.

[22] Dharaskar, R., Patil, S., & Thakare, V. (2017). Digital Forensic in Cloud: Critical Analysis of Threats and Security in IaaS, SaaS and PaaS and Role of Cloud Service Providers. In International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 17–18 August (pp. 1–7). India: IEEE.

[23] Erlin, E., Lizarti, N., & Sudyana, D. (2013) Forensic Investigation Framework on Server Side of Private Cloud Computing. Lontar Komputer: Jurnal Ilmiah Teknologi Informasi, 181-192. Gladyshev, P., James, J. I. (2016). A survey of mutual legal assistance involving digital evidence, Digital Investigation, 18, 23–32. doi.org/10.1016/j.diin.2016.06.004

[24] Gritzalis, S., Kalloniatis, C., Katos, V., & Simou, S. (2019). A Revised Forensic Process for Aligning the Investigation Process with the Design of Forensic-Enabled Cloud Services. In K. Sokratis, & V. Zorkadis (Eds.), E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age: 8th International Conference, e-Democracy 2019, Athens, Greece, 12–13 December (161–177). Cham: Springer.

[25] Hurst, M. R., Herman, M., Iorga, M., Jackson, R. H., Leo, R., Salim, A. M., ... Sardinas, R. (2020). NIST Cloud Computing Forensic Science Challenges, 1-80, doi:10.6028/NIST.IR.8006

[26] Horsman, G. (2020). What's in the Cloud - An Examination of the Impact of Cloud Storage Usage on the Browser Cache. The Journal of Digital Forensics, Security and Law, 15(1), 1-16, doi:10.15394/jdfsl.2020.1592

[27] Jõgi, L., Kaldoja, K., Luuk, M., Randma H., (2018). Need for Speed in Mutual Legal Assistance', European

Judicial Training Network – EJTN: 13th edition of the THEMIS Competition. Retrieved on July 7, 2020 from http://www.ejtn.eu/PageFiles/17290/WR\%20TH-2018-01\%20EE.pdf

[28] Karatysz, M. (2013) Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski, Refleksje, 7, 139-149. Karie, N. M., & Karume, S. (2017). Digital Forensic Readiness in Organizations: Issues and Challenges. The Journal of Digital Forensics, Security and Law, 12(4), 43-54. doi:10.15394/jdfsl.2017.1436

[29] Horng, G., Huang CT, Ko, HJ., Wang, SJ., & Zhuang ZW. (2021). Cloud Evidence Tracks of Storage Service Linking with IOS Systems. The Journal of Supercomputing, 77(1), 77-94. doi:10.1007/s11227-020-03255-5

[30] Mohammed, K. H., Mohammed,Y. D. & Solanke A. A. (2019). Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 56-63.

[31] Mahanamahewa, P., & Perera, P. (2017). Analysis of Dependencies & Legal Barriers on Digital Forensic Investigations in Sri Lanka. KDU E – Repository. Retrieved on January 21, 2021 from http://ir.kdu.ac.lk/handle/345/1733.

[32] Mohiddin, S. K., Sharmila S. & Yalavarthi S. B. (2017). A Complete Ontological Survey of Cloud Forensic in the Area of Cloud Computing. In K. Deep, J. C.

[33] Bansal, K. N. Das, A. K. Lal, H. Garg, A. K. Nagar & M. Pant (Eds.), Proceedings of Sixth International Conference on Soft Computing for Problem Solving: Advances in Intelligent Systems and Computing 546. Lviv, Ukraine, 6–10 September (pp. 38-47). Singapore: Springer.

[34] Olber, P. 2019. Survey on cross-border collection of digital evidence from cloud computing. Retrieved on June 20, 2020 from https://osf.io/mwxu6Opitek, P. (2018) Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych, Prokuratura i Prawo, 7/8, 65-85.

[35] Osula, A. M., Zoetekouw, M. (2017). The notification requirement in transborder remote search and seizure: domestic and international law perspectives, Masaryk University Journal of Law and Technology, 13(2), 103-127, doi.org/10.5817/MUJLT2017-1-6

[36] Seger, A. (2013, November 1). Capacity building on cybercrime – discussion paper. Council of Europe, Strasbourg, pp. 1-29.

[37] Trenwith, P. M., & Venter, H. S. (2019). FReadyPass: a digital forensic ready passport to control access to data across jurisdictional boundaries. Australian Journal of Forensic Sciences, 51(5), 583-595. doi:10.1080/00450618.2018.1444090

[38] Wang, H., He, W., & Wang, F. K. (2012). Enterprise cloud service architectures. Information Technology and Management, 13(4), 445-454. doi:10.1007/s10799-012-0139-4

Appendices

For interested readers a detailed survey results are presented in the Appendices: 1–4.

Table 2. Appendix 1. Practical-related questions.

		Prosecutor's office		Court		Total		Test Chi-2	
		N	%	N	%	N	%	Chi 2	p
Q1. Experience in collecting evidence from the cloud.									
1	Yes	14	24.1%	3	3.7%	17	12.2%	13.147	0.000
2	No	44	75.9%	78	96.3%	122	87.8%	Cramer's	
3	Total	58	100.0%	81	100.0%	139	100.0%	V=0.308	
Q2. Used procedure and type of procedural act.									
1	Legal decision to request data	4	4.9%	1	1.2%	5	3.6%	3.373	0.066
2	Search of an IT system	4	4.9%	0	0.0%	4	2.9%	5.069	0.014
3	Mutual legal assistance	2	2.5%	0	0.0%	2	1.4%	2.959	0.054
4	Appointing an IT expert	1	1.2%	1	1.2%	2	1.4%	0.077	0.781
5	Visual inspection	0	0.0%	1	1.2%	1	0.7%	0.684	0.408
6	Obtaining data and logging	1	1.2%	0	0.0%	1	0.7%	1.484	0.223
Q3. Opinion on whether gathering digital evidence from clouds is a problem?									
1	Yes	28	48.3%	23	28.4%	51	36.7%	7.651	0.022
2	No	5	8.6%	4	4.9%	9	6.5%	Cramer's	
3	Don't know / Hard to say	23	43.1%	54	66.7%	79	56.8%	V=0.235	
4	Total	58	100.0%	81	100.0%	139	100.0%		
Q4. Identified problems:									
1	Ineffective cooperation	7	12.1%	9	11.1%	16	11.5%	0.050	0.824
2	Voluntary help of CSPs	9	15.5%	7	8.6%	16	11.5%	1.761	0.192
3	Lack of procedures	6	10.3%	6	7.4%	12	8.6%	0.423	0.515
4	Different legal systems	5	8.6%	1	1.2%	6	4.3%	4.606	0.032
5	Lack of knowledge	2	3.4%	4	4.9%	6	4.3%	0.159	0.690
6	Servers out of the country	0	0.0%	5	6.2%	5	3.6%	3.634	0.057
7	CSP out of country	3	5.2%	2	2.5%	5	3.6%	0.759	0.384
8	Lack of tools	2	3.4%	2	2.5%	4	2.9%	0.132	0.716
9	Various data retention time	2	3.4%	1	1.2%	3	2.2%	0.823	0.364
10	Anti-forensic	1	1.7%	1	1.2%	2	1.4%	0.063	0.798
11	Determination of the offender	0	0.0%	1	1.2%	1	0.7%	0.705	0.401
Q5. Proposed solutions:									
1	New effective law	5	8.6%	5	6.2%	10	7.2%	0.303	0.582
2	Training	4	6.9%	3	3.7%	7	5.0%	0.720	0.396
3	Improved cooperation	5	8.6%	0	0.0%	5	3.6%	7.243	0.007
4	Establishment of procedures	3	5.2%	2	2.5%	5	3.6%	0.712	0.399
5	Increase the budget	1	1.7%	1	1.2%	2	1.4%	0.057	0.811
6	Improving cooperation	0	0.0%	2	2.5%	2	1.4%	1.453	0.228
7	Direct work with CSPs	2	3.4%	0	0.0%	2	1.4%	2.834	0.092
8	Unification of legal systems	2	3.4%	0	0.0%	2	1.4%	2.834	0.092

Table 3. Appendix 2. Cloud Service Provider-related questions.

		Prosecutor's office		Court		Total		Test Chi-2	
		N	%	N	%	N	%	Chi 2	p
Q1. Experience in collecting evidence from the cloud.									
1	Yes	14	24.1%	3	3.7%	17	12.2%	13.147	0.000
2	No	44	75.9%	78	96.3%	122	87.8%	Cramer's	
3	Total	58	100.0%	81	100.0%	139	100.0%	V=0.308	
Q2. Used procedure and type of procedural act.									
1	Legal decision to request data	4	4.9%	1	1.2%	5	3.6%	3.373	0.066
2	Search of an IT system	4	4.9%	0	0.0%	4	2.9%	5.069	0.014
3	Mutual legal assistance	2	2.5%	0	0.0%	2	1.4%	2.959	0.054
4	Appointing an IT expert	1	1.2%	1	1.2%	2	1.4%	0.077	0.781
5	Visual inspection	0	0.0%	1	1.2%	1	0.7%	0.684	0.408
6	Obtaining data and logging	1	1.2%	0	0.0%	1	0.7%	1.484	0.223
Q3. Opinion on whether gathering digital evidence from clouds is a problem?									
1	Yes	28	48.3%	23	28.4%	51	36.7%	7.651	0.022
2	No	5	8.6%	4	4.9%	9	6.5%	Cramer's	
3	Don't know / Hard to say	23	43.1%	54	66.7%	79	56.8%	V=0.235	
4	Total	58	100.0%	81	100.0%	139	100.0%		
Q4. Identified problems:									
1	Ineffective cooperation	7	12.1%	9	11.1%	16	11.5%	0.050	0.824
2	Voluntary help of CSPs	9	15.5%	7	8.6%	16	11.5%	1.761	0.192
3	Lack of procedures	6	10.3%	6	7.4%	12	8.6%	0.423	0.515
4	Different legal systems	5	8.6%	1	1.2%	6	4.3%	4.606	0.032
5	Lack of knowledge	2	3.4%	4	4.9%	6	4.3%	0.159	0.690
6	Servers out of the country	0	0.0%	5	6.2%	5	3.6%	3.634	0.057
7	CSP out of country	3	5.2%	2	2.5%	5	3.6%	0.759	0.384
8	Lack of tools	2	3.4%	2	2.5%	4	2.9%	0.132	0.716
9	Various data retention time	2	3.4%	1	1.2%	3	2.2%	0.823	0.364
10	Anti-forensic	1	1.7%	1	1.2%	2	1.4%	0.063	0.798
11	Determination of the offender	0	0.0%	1	1.2%	1	0.7%	0.705	0.401
Q5. Proposed solutions:									
1	New effective law	5	8.6%	5	6.2%	10	7.2%	0.303	0.582
2	Training	4	6.9%	3	3.7%	7	5.0%	0.720	0.396
3	Improved cooperation	5	8.6%	0	0.0%	5	3.6%	7.243	0.007
4	Establishment of procedures	3	5.2%	2	2.5%	5	3.6%	0.712	0.399
5	Increase the budget	1	1.7%	1	1.2%	2	1.4%	0.057	0.811
6	Improving cooperation	0	0.0%	2	2.5%	2	1.4%	1.453	0.228
7	Direct work with CSPs	2	3.4%	0	0.0%	2	1.4%	2.834	0.092
8	Unification of legal systems	2	3.4%	0	0.0%	2	1.4%	2.834	0.092

Table 4. Appendix 3. 24/7 contact point-related questions.

		Prosecutor's office		Court		Total		Test Chi-2	
		N	%	N	%	N	%	Chi 2	p
Q1. Experience in collecting evidence from the cloud.									
1	Yes	14	24.1%	3	3.7%	17	12.2%	13.147	0.000
2	No	44	75.9%	78	96.3%	122	87.8%	Cramer's	
3	Total	58	100.0%	81	100.0%	139	100.0%	V=0.308	
Q2. Used procedure and type of procedural act.									
1	Legal decision to request data	4	4.9%	1	1.2%	5	3.6%	3.373	0.066
2	Search of an IT system	4	4.9%	0	0.0%	4	2.9%	5.069	0.014
3	Mutual legal assistance	2	2.5%	0	0.0%	2	1.4%	2.959	0.054
4	Appointing an IT expert	1	1.2%	1	1.2%	2	1.4%	0.077	0.781
5	Visual inspection	0	0.0%	1	1.2%	1	0.7%	0.684	0.408
6	Obtaining data and logging	1	1.2%	0	0.0%	1	0.7%	1.484	0.223
Q3. Opinion on whether gathering digital evidence from clouds is a problem?									
1	Yes	28	48.3%	23	28.4%	51	36.7%	7.651	0.022
2	No	5	8.6%	4	4.9%	9	6.5%	Cramer's	
3	Don't know / Hard to say	23	43.1%	54	66.7%	79	56.8%	V=0.235	
4	Total	58	100.0%	81	100.0%	139	100.0%		
Q4. Identified problems:									
1	Ineffective cooperation	7	12.1%	9	11.1%	16	11.5%	0.050	0.824
2	Voluntary help of CSPs	9	15.5%	7	8.6%	16	11.5%	1.761	0.192
3	Lack of procedures	6	10.3%	6	7.4%	12	8.6%	0.423	0.515
4	Different legal systems	5	8.6%	1	1.2%	6	4.3%	4.606	0.032
5	Lack of knowledge	2	3.4%	4	4.9%	6	4.3%	0.159	0.690
6	Servers out of the country	0	0.0%	5	6.2%	5	3.6%	3.634	0.057
7	CSP out of country	3	5.2%	2	2.5%	5	3.6%	0.759	0.384
8	Lack of tools	2	3.4%	2	2.5%	4	2.9%	0.132	0.716
9	Various data retention time	2	3.4%	1	1.2%	3	2.2%	0.823	0.364
10	Anti-forensic	1	1.7%	1	1.2%	2	1.4%	0.063	0.798
11	Determination of the offender	0	0.0%	1	1.2%	1	0.7%	0.705	0.401
Q5. Proposed solutions:									
1	New effective law	5	8.6%	5	6.2%	10	7.2%	0.303	0.582
2	Training	4	6.9%	3	3.7%	7	5.0%	0.720	0.396
3	Improved cooperation	5	8.6%	0	0.0%	5	3.6%	7.243	0.007
4	Establishment of procedures	3	5.2%	2	2.5%	5	3.6%	0.712	0.399
5	Increase the budget	1	1.7%	1	1.2%	2	1.4%	0.057	0.811
6	Improving cooperation	0	0.0%	2	2.5%	2	1.4%	1.453	0.228
7	Direct work with CSPs	2	3.4%	0	0.0%	2	1.4%	2.834	0.092
8	Unification of legal systems	2	3.4%	0	0.0%	2	1.4%	2.834	0.092

Table 5. Appendix 4. Opinion and knowledge-related questions.

		Prosecutor's office		Court		Total		Test Chi-2	
		N	%	N	%	N	%	Chi 2	p
Q16. Familiarity with initiatives to improve procedures to get digital evidence from clouds.									
1	Yes	2	3.4%	1	1.3%	3	2.2%		
2	No	56	96.6%	79	98.7%	135	97.8%	0.764	0.382
3	Total	58	100.0%	80	100.0%	138	100.0%		
Q17. Indicated initiatives.									
1	EIO exchange system	1	1.7%	0	0.0%	1	0.7%	1.407	0.236
2	EIO	0	0.0%	1	1.2%	1	0.7%	0.721	0.396
Q18. Attendance at training on collecting digital evidence from clouds.									
1	Yes	6	10.3%	3	3.7%	9	6.5%		
2	No	52	89.7%	78	96.3%	130	93.5%	2.462	0.117
3	Total	58	100.0%	81	100.0%	139	100.0%		
Q19. Attendance at training on cloud computing technologies.									
1	Yes	6	10.3%	3	3.7%	9	6.5%		
2	No	52	89.7%	78	96.3%	130	93.5%	2.462	0.117
3	Total	58	100.0%	81	100.0%	139	100.0%		
Q20. Courses in which the respondents took part .									
1	Combating cybercrime	5	8.6%	2	2.5%	7	5.0%	2.760	0.097
2	Cybercrime and jurisdiction	1	1.7%	0	0.0%	1	0.7%	1.457	0.227
3	Cross-border drug crime	0	0.0%	1	1.2%	1	0.7%	0.709	0.400
4	Post-graduate studies	0	0.0%	1	1.2%	1	0.7%	0.709	0.400
Q21. The view that the Polish Police have the authority remotely search an information system.									
1	Yes	13	22.4%	27	33.3%	40	28.8%	9.321	0.009
2	No	11	19.0%	3	3.7%	14	10.1%		
3	Don't know / Hard to say	34	58.6%	51	63.0%	85	61.2%	Cramer's	
4	Total	58	100.0%	81	100.0%	139	100.0%	V=0.259	
Q22. Awareness whether searching the content of an e-mail inbox complies with the law.									
1	Yes	30	51.7%	26	32.1%	56	40.3%		
2	No	4	6.9%	8	9.9%	12	8.6%	5.412	0.067
3	Don't know / Hard to say	24	41.4%	47	58.0%	71	51.1%		
4	Total	58	100.0%	81	100.0%	139	100.0%		
Q23. Types of procedural activities on which to search the contents of e-mails.									
1	Visual examination	19	32.8%	26	32.1%	45	32.4%	0.023	0.879
2	Search of an IT system	19	32.8%	12	14.8%	31	22.3%	6.587	0.010
3	Forensic expertise	3	5.2%	6	7.4%	9	6.5%	0.252	0.615
4	Procedural control	3	5.2%	0	0.0%	3	2.2%	4.358	0.023
5	Experimental reconstruction	1	1.7%	0	0.0%	1	0.7%	1.431	0.232
Q24. Legality in obtaining electronic evidence from the cloud.									
1	Crime scene	20	34.5%	20	24.7%	40	28.8%	0.816	0.366
2	Don't know/Hard to say	10	17.2%	29	35.8%	39	28.1%	5.501	0.025
3	Location of CSP HQ	11	19.0%	11	13.6%	22	15.8%	1.757	0.185
4	Location of stored data	10	17.2%	9	11.1%	19	13.7%	1.166	0.280
5	Location of the owner	3	5.2%	10	12.3%	13	9.4%	1.967	0.161
6	Location of the offender	6	10.3%	6	7.4%	12	8.6%	0.410	0.525
7	Location of service offering	4	6.9%	5	6.2%	9	6.5%	0.039	0.843
8	Location of the victim	3	5.2%	6	7.4%	9	6.5%	0.252	0.615
9	Place of CSP's representative	3	5.2%	4	4.9%	7	5.0%	0.097	0.932
Q25. Basis for remote search or other means of remote access to data.									
1	Don't know / Hard to say	23	39,7%	40	49,4%	63	45,3%	0,754	0,385
2	Publicly available data	13	22,4%	18	22,2%	31	22,3%	0,037	0,841
3	Person's consent	9	15,5%	18	22,2%	27	19,4%	0,707	0,401
4	Service provider in a country that has ratified the CETS	7	12,1%	15	18,5%	22	15,8%	0,810	0,368
5	Inability to specify service provider	8	13,8%	7	8,6%	15	10,8%	1,163	0,281
6	Procedural control	7	12,1%	7	8,6%	14	10,1%	0,592	0,442
7	No knowledge of data location	3	5,2%	5	6,2%	8	5,8%	0,031	0,861
8	Uncertainty of data location	3	5,2%	5	6,2%	8	5,8%	0,031	0,861