DR RAFAŁ WIELKI
University of Opole | DOI: 10.32041/9788367149761/9

Chapter 9. Data Retention and Legal Problems of Investigating Cybercrime

9.1. Introduction

Investigating cybercrimes certainly requires the proper technical and substantive preparation of law enforcement agencies, but public services operate primarily on the basis and within the limits of the law. In view of the above, effective investigative activities require a proper legal basis, and there is no denying that legal regulations often have not kept pace with changes in social and technological reality.

The purpose of this chapter is to present the formation of data retention law in the European Union, as well as the problems that lawmakers have encountered over time, which were related to the position of the Court of Justice of the European Union.

Another goal is to show how Polish services operate under the law and how they obtain retention data from Internet Service Providers, while discussing the controversies that arise among lawyers.

Further considerations will be related to proposed changes at the European Union level, which may result in greater accountability of Internet Service Providers for the content they share, as well as the data they process. Finally, another problem touches on legal issues, as an answer is sought to the questions of what legal acts regulate data retention, whether existing national and international regulations are effective and whether they require possible changes, as well as in what direction these changes should go.

9.2. Law on Data Retention in European Union

Problems related to the effective prosecution of cybercrime are also grounded in the law, as many areas are not normalised in either national or international regulations. The aim of this part is to present the problem of data retention by operators of means of electronic communication in order to ensure public security. Effective investigation and combating cybercrime requires access to this data, however, it is presumed that current national as well as international regulations may not meet the needs of the services. It is necessary to reflect on the authorities authorised to access retention data, as well as to define balanced boundaries between fighting cybercrime and ensuring respect for human rights and freedoms.

We should start by considering the first piece of legislation that comprehensively addressed cybercrime, and we are referring to the Convention on Cybercrime, [1] which concerns the prevention of crimes related to the use of new technologies and aims to improve public safety in virtual space. Incidentally, it is worth adding that the Convention was ratified by Hungary in 2003, while it was not ratified by Poland until 2015. Thus, the primary purpose of the Convention was to introduce a uniform catalogue of criminal acts committed by users of information networks, to establish specific procedures for the detection and prosecution of cybercrime, and to set standards for international cooperation in this field.

These goals can be considered achieved. The Convention introduces a catalogue of types of crimes committed using computer systems. These include computer fraud, computer forgery, the crime of hacking (among others, illegal access to a computer system, as well as the manufacture or sale of "hacking tools"), dissemination, possession of child pornography, or copying and distribution of works protected by intellectual property rights. The Cybercrime Convention also requires parties to adopt appropriate procedural arrangements that are necessary for the purposes of ongoing criminal proceedings for the crimes specified in the Convention and are intended

[1] Convention on Cybercrime (ETS No. 185), Budapest 23/11/2001 – Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States.

to help authorised national authorities identify perpetrators and collect evidence of their acts. Among other things, the treaty introduces rules and guarantees for searches of computer resources or the transfer, sharing and safeguarding of computer data. The Convention also obliges parties to introduce appropriate legal measures to strengthen international cooperation in combating cybercrime through, among other things, the provision of legal assistance (including data exchange) or extradition of perpetrators. Over time, the Convention has been modernised through additional protocols on the criminalisation of racist and xenophobic acts[2] and cooperation and disclosure of electronic evidence.[3]

Importantly, the Convention addresses the problem of data retention on a baseline basis. According to Article 20(1) of the Convention:

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to collect or record through the application of technical means on the territory of that Party, and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party; or to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

Further reference to data retention is found in Article 21(1) of the Convention:

> Each Party shall adopt such legislative and other measures as may be necessary, in relations to a range of serious offences to be determined by domestic law, to empower

[2] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

[3] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

> its competent authorities to: collect or record through the application of technical means on the territory of that Party, and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party, or to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system'.

These regulations are not able to completely normalise the problem of data retention, hence attempts have been made on the ground in the European Union to clarify regulations that would allow law enforcement agencies to access data on network traffic collected by ICT network operators. Hence, the following were put into effect Directive 2006/24/EC of the European Parliament and of the Council.[4] The directive imposed an obligation on providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed by those providers. This obligation applied to both telephone and Internet connections and covered a wide range of data necessary for:

- determine the source of the call, including the name and address of the user(subscriber),
- determining the recipient of the call, including the user(subscriber)'s number or ID, name and address,
- determining the date, time and duration of the call,
- determining the type of call,
- communication tool,
- identification of the location of the mobile communication device.

[4] Directive 2006/24/EC of the European Parliament and of the Council of March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

However, this directive has been challenged by the Court of Justice of the European Union.[5] The proceedings were initiated on the basis of a request for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (TFEU) from the High Court of Ireland and the Verfassungsgerichtshof of Austria. The reference for a preliminary ruling arose in connection with a complaint by Digital Rights Ireland Ltd, in which the legality of national legislation on the retention of data related to electronic communications was challenged. The source for the proceedings before the CJEU was also a second complaint by the Carinthian national government and several thousand individuals also concerning the compatibility of Directive 2006/24/EC with the EU Charter of Fundamental Rights. The contradiction was limited to the extent to which Directive 2006/24/EC allows the mass collection over a long period of time of various types of data on an unlimited number of individuals. The complaints argued that the scope of the obligations imposed and the associated restrictions on rights are disproportionate, and are not necessary or are inadequate for legitimate purposes, i.e., to ensure the availability of data for the detection, conduct and prosecution of serious crimes or to ensure the proper functioning of the EU internal market. According to the ruling, in accordance with the principle of proportionality, legal acts of the European Union should contain provisions adequate to achieve the legitimate objectives they are intended to serve and should not go beyond what is necessary to achieve those objectives.[6]

9.3. Polish Approach to Data Retention

There is no doubt that the judgment discussed above has strongly influenced the shape of the proposed legislation, while at the same time provoking – at long last – legitimate discussions about the limit

[5] Judgment of the Court of European Union of 8 April 2014, C-293/12 and C-594/12.

[6] M. Wach, *Dalsze losy retencji danych po wyroku Trybunału Sprawiedliwości UE,* "Ius Novum" 2016, nr 3, p. 200.

of violating civil liberties in the name of combating threats to public security. The verdict has resulted in an approach such that the general and mass storage of mobile or Internet users' traffic and location data is allowed only in the case of a serious threat to national security, and is unlikely to be the rule. However, it should be noted that at the beginning of the new millennium, the world was shaken by successive reports of terrorist attacks, and extreme terrorist groups and organisations had a real impact on the policies pursued in many countries. Nowadays, a greater understanding of civil liberties tends to be shown, but the steady growth of cybercrime must not influence the complete abandonment of data retention, as this would tie the hands of investigators throughout the European Union.

Data retention issues are of interest to the European Union and national legislators. This is particularly relevant, so it is to be expected that data retention issues will be regulated at this level, as was the case with personal data regulated by the General Data Protection Regulation.[7] Currently in Poland there is a discussion on the shape of national data retention laws, as there is a dispute among lawyers about the compatibility of current legal norms with European Union law. The Ombudsman stresses that data collection should be limited to fighting major crimes and should be controlled by an independent body; and the citizen should find out that he or she has been so invigilated. Meanwhile, today the courts actually check this post factum on the basis of general reports from the services – as a result, they cannot reliably assess the legitimacy, adequacy and expediency of these activities. In turn, according to the Ministry of Internal Affairs and Administration, the current legislation does not violate the requirement of proportionality of interference with the right to privacy, freedom of communication and informational autonomy. In the ministry's view, on the other hand, restricting access to telecommunications data will undoubtedly make it much more difficult to detect perpetrators of crimes.

[7] See: Regulation (EU) 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Let's take a look at the Police Act, for example.[8] According to Article 20c, for the purpose of preventing or detecting crimes, fiscal offences, or for the purpose of saving human life or health or supporting search and rescue operations, the police may obtain data not constituting the content of a telecommunications transmission, a postal consignment, or a transmission within the framework of an electronically provided service, respectively – as defined in specific provisions – and may process them without the knowledge and consent of the subject. These are data necessary to:

- determine the network termination, the telecommunications terminal equipment, the end user initiating the call to which the call is directed,
- determine the date and time of the call and its duration, the type of call, the location of the telecommunications terminal equipment,
- obtain data about the postal operator, the postal services provided, and information that allows identification of the users of these services, and:
  - surname and first names of the recipient of the service,
  - PESEL registration number or, if this number has not been assigned, the number of the passport, identity card or other document confirming identity,
  - address of permanent residence registration,
  - correspondence address, if different from the address referred to in item 3,
  - data used to verify the electronic signature of the service recipient,
  - electronic addresses of the service recipient,
  - designations identifying the service recipient assigned on the basis of the data,
  - designations identifying the termination of the telecommunications network or data communications system used by the service recipient,
  - information about the beginning, end and scope of each use of the electronically provided service,

[8] Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. 2023 poz. 171).

– information on the use of electronically provided services by the recipient.

It can be noted that in Polish regulations, the scope of data that can be obtained by the police without judicial supervision of pre-trial proceedings is relatively large, which is why it raises so much controversy and provokes discussions among lawyers.

9.4. Some Comments about the Future

The EU is implementing the Digital Services Act (DSA) and the Digital Markets Act (DMA),[9] which are expected to include regulations for platforms and ways to combat harmful or illegal content online. The EU's efforts are moving in the direction of regulating the Internet through regulations, rather than rules and regulations set by platforms, but it will emphasise that these regulations must protect freedom of expression and fundamental rights, avoiding censorship. And there is undoubtedly a need for regulations governing data retention by social media owners and the release of such data to investigators on the basis of EU regulations, rather than internal rules and regulations, as is often the case today.

The DSA applies to Internet intermediary services, which are used by millions of Europeans every day. The obligations of various online entities have been defined according to their role, market share and power of influence on the online ecosystem. The new EU rules will have to be complied with by all online intermediaries offering their services in the single market, regardless of whether they are based inside or outside the EU. The obligations of micro and small businesses will be proportional to their performance and market share, which does not mean they will be exempt from liability. These regulations should be viewed very positively, as up to now the Internet giants have often refused to cooperate, including in crime-fighting efforts. The Digital Services Act significantly

[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

improves mechanisms for removing illegal content and effectively protecting users' fundamental rights on the Internet, including freedom of expression. It also increases the level of public control over the activities of online platforms.

The DMA establishes strictly defined objective criteria for qualifying a large online platform as an "access gatekeeper" (controlling access to information and services). This ensures that the act remains well-targeted to the problem of large, systemic Internet platforms. Access gatekeepers will retain all opportunities to innovate and offer new services. However, they will no longer benefit unduly, as they will no longer be able to engage in unfair practices against business users and customers who depend on them. Platforms will have to allow third parties to interact with their own access gatekeeper services in certain specific situations, or allow their business users to access the data they generate when using the access gatekeeper platform.

It is worth noting that several pieces of legislation are under development at the EU level, and one of the most important in the context of cyber security is the Network and Information Security Directive (NIS2).[10] The NIS 2 proposal expands the scope of NIS by requiring more entities and sectors to take appropriate action, including providers of public electronic communications services, social media operators, manufacturers of critical products (e.g., medical devices), and postal and courier services. NIS2 also strengthened security requirements, addressed the cybersecurity of supply chains, simplified reporting obligations, and introduced more stringent supervisory measures and enforcement requirements, including harmonised sanctions. In addition, a network of cyber security crisis liaison organisations (EU-CyCLONe) has been established.

It has also been noted that EU law pays little attention to operational risks related to information and communications technology (ICT). In September 2020, the Commission presented a proposal for

[10] European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM (2020)0823 – C9-0422/2020 – 2020/0359(COD)).

a regulation on the operational digital resilience of the financial sector (DORA),[11] to introduce and harmonise key digital operational requirements across the EU to ensure the resilience of ICT operations in the event of major operational disruptions and cyberattacks. The proposed Digital Operational Resilience Act (DORA) is designed to ensure that EU financial sector operations are able to withstand operational disruptions and cyberattacks. It provides a framework governing operational digital resilience, under which all companies must make sure they can withstand, respond to and overcome all types of ICT-related disruptions and threats. The proposed regulation covers a wide range of financial institutions, including credit institutions, payment institutions and electronic money institutions, crypto-asset service providers, central securities depositories, trading venues and trade repositories. If the DORA proposal is formally adopted, the relevant European supervisory authorities will develop technical standards to regulate all financial services institutions. Implementation will be supervised and enforced by the relevant national authorities. The package is intended to foster innovation and the spread of new financial technologies, while providing an environment that guarantees an appropriate level of protection.

In conclusion, it seems that currently the problem of data retention in the law is present and needs further resolution. After the already discussed judgment of the Court of Justice of the EU, data retention issues have been set aside, so to speak, pointing to possible violations of civil liberties, which in practice means that member states regulate data retention issues individually, more or less following the CJEU ruling.[12] This state of affairs is not conducive to combating cybercrime, which is cross-border in nature, and effectively combating it requires harmonisation of regulations over a larger area, albeit the European Union, although it would be

[11] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

[12] See: European Union Agency for Fundamental Rights, *Data retention across the EU*, https://fra.europa.eu/en/publication/2017/data-retention-across-eu (accessed on: 30.07.2023).

worthwhile to develop solutions with an even broader territorial scope. The regulations introduced so far, however, may gradually bring about evolutionary changes in the approach to data processing, which over time will take into account the balance between civil liberties and law enforcement needs.

9.5. Conclusions

In view of the above, it is postulated that work should begin on the obligation of data retention by Internet Service Providers, which are most often counted among the Internet giants, and the regulation of their activities within the European Union and cooperation with law enforcement agencies. Nowadays, it is very difficult to obtain data on suspected social media users, and to a large extent, obtaining data by investigators depends on the will of service providers, who hide behind the fact that they operate outside the European Union and thus are not subject to European jurisdiction. By failing to cooperate with law enforcement in sharing traffic data on suspected users, online platforms are essentially making it easier for cybercriminals to go unpunished.

Perhaps the most important issue, which is an extension of the previously mentioned topic, is the general issue of data retention and legislation in this regard. Within the European Union, there is a problem with international cooperation on the fight against cybercrime due to the current legislation. The initial direction of what data should be collected and how it should be collected was determined by Directive 2006/24/EC of the European Parliament and of the Council, but as we mentioned, it was challenged by the Court of Justice of the European Union, which argued that the scope of the obligations imposed and the related restrictions on rights are disproportionate, and are not necessary or are inappropriate for legitimate purposes, i.e., to ensure the availability of data for the detection, conduct and prosecution of serious crimes or to ensure the proper functioning of the EU internal market.

According to the ruling, according to the principle of proportionality, European Union acts should contain provisions that are adequate

to achieve the legitimate objectives they are intended to serve and should not go beyond what is necessary to achieve those objectives. Since then, despite the introduction of many regulations that indirectly refer to the retention of telecommunications, postal data, etc., there is still a lack of legislation that regulates this issue directly.

In Poland, although there are partial regulations that give some services access to data and that force service providers to retain data, indicating the duration of storage of knowledge held, they are the subject of a dispute among lawyers, and there is still no consensus on establishing data retention rules in relation to civil liberties, and thus no balance is achieved.

The laws in force in the various EU countries are not uniform, which is not conducive to the exchange of information that is so necessary to combat cross-border cybercrime. It seems high time to raise the need for renewed discussion among member states on the creation of a legal act that would give a framework to and address the issue of civil liberties on the one hand and the needs of investigators who need access to data on the other.

REFERENCES

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

Convention on Cybercrime (ETS No. 185), Budapest 23/11/2001 – Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States.

Directive 2006/24/EC of the European Parliament and of the Council of March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

European Union Agency for Fundamental Rights, *Data retention across the EU*, https://fra.europa.eu/en/publication/2017/data-retention-across-eu (accessed on: 30.07.2023).

European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM (2020)0823 – C9-0422/2020 – 2020/0359(COD)).

Judgment of the Court of European Union of 8 April 2014, C-293/12 and C-594/12.

Regulation (EU) 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. 2023 poz. 171).

Wach, M., *Dalsze losy retencji danych po wyroku Trybunału Sprawiedliwości UE,* "Ius Novum" 2016, No. 3, p. 200.