THEMIS Competition Semi-final A

EU and European Criminal Law

Assistant Prosecutor Ange Kangur

Assistant Prosecutor Karin Orgulas

Assistant Prosecutor Iris Asuküla

Data Retention - a Clash Between Liberty and Security

Tutor

Katrin Paesoo

Estonia

2022

Introduction

One of the leading positions currently held by many legal experts is that communication data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[1]

The above position of the Court of Justice of the European Union (hereinafter CJEU) has been the subject of most data related discussions since the European Parliament and Council of Europe adopted the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks in March 15, 2006.[2]

Legislators and constitutional courts of several Member States of the European Union (hereinafter Member States) were of the position that retaining communication data and transferring data to the authorities constitutes an unjustified encroachment on fundamental rights. Therefore, Member States such as Ireland, Greece, Sweden and Austria did not adopt the laws, regulations and administrative provisions necessary to comply with Directive 2006/24/EC, which is the reason why CJEU reached a decision in 2009[3] that the mentioned Member States have failed to fulfil their obligations under that directive and ordered them to pay the costs.

CJEU declared the Directive 2006/24/EC invalid in 2014 in its landmark decision *Digital Rights Ireland and Seitlinger*[4], mainly because Directive 2006/24/EC covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

---

[1] Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238), at para. 27.
[2] Directive of the European Parliament and of the Council 2006/24, OJ 2006 L 105/54.
[3] Case C-202/09, *Commission of the European Communities v Ireland* (EU:C:2009:736); Case C-211/09, *Commission of the European Communities v Hellenic Republic* (EU:C:2009:737); Case C-185/09, *European Commission v Kingdom of Sweden* (EU:C:2010:59); Case C-189/09, *European Commission v Republic of Austria* (EU:C:2010:455).
[4] Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238).

After declaring the Directive 2006/24/EC invalid, the European Commission gave a statement that the Commission is not coming forward with any new initiatives on Data Retention: "*in the absence of European Union rules, Member States are free to maintain their current data retention systems or set up new ones, providing of course they comply with basic principles under EU law, such as those contained in the ePrivacy Directive*".[5]

The aforementioned statement did not solve the problem - despite the extensive instructions given in decision *Digital Rights Ireland and Seitlinger*, there was no common understanding at the national level of Member States as to how these judgements and their consequences should be interpreted. *Vice versa*, to this day there is too much room for interpretation. This has led to a situation where many requests for preliminary rulings about the interpretation of European Union (hereinafter EU) law have been made to the CJEU. To this day questions regarding data retention, making data available to the authorities and the relationship between data retention and fundamental rights stated in the Charter of Fundamental Rights (hereinafter the Charter) have risen in many Member States.

Estonia adopted the laws to comply with Directive 2006/24/EC. After CJEU declared the Directive 2006/24/EC invalid in 2014, Estonian legislators maintained the data retention systems in compliance with the invalid Directive, despite the fact that a lot of questions were raised whether the law in force complies with basic principles under EU law, such as those contained in the ePrivacy Directive (2002/58/EC).[6] These problems were not solved until the Supreme Court of Estonia requested preliminary ruling about the interpretation of EU law from CJEU on November 12, 2018.[7]

On 2 March 2021, the CJEU shed more light on this matter in response to a request for preliminary ruling submitted by the Supreme Court of Estonia. This decision led to a situation where there was no chance to get access to any communication data at all in criminal

[5] Commission Statement of 16 September 2015, OJ 2015 L15/5654.
[6] Virks, "Sideandmed ja nende säilitamise olulisus", 8 Juridica (2018) 581, at 586.
[7] Supreme Court of Justice of Estonia 1-16-6179.

proceedings, because the laws in force were not in accordance with the opinions held by the CJEU.

On 1 January 2022, an amendment to the Code of Criminal Procedure of Estonia (hereinafter CCP)[8] entered into force. In particular, the amended law concerned requiring data from electronic communication undertakings. Before January 1, 2022 the CCP provided that the Prosecutor's Office may give a permission to the investigative body to make enquiries in pre-court procedure about the data listed in subsections 2 and 3 of § 111^1 of the Electronic Communications Act (hereinafter ECA). After the amendment, CCP provided that the authorisation of the pre-trial investigation judge is necessary to make the aforementioned enquiries.

Still, there is a lot of confusion regarding the communication data requests and data retention in Estonia and probably in other Member States as well, which is why the authors discuss the topic in this paper and try to discuss some problems and offer their own solutions to some of the problems that have arisen, focusing mainly on data retention and protecting public security in Member States.

Firstly, the authors focus on EU legislation, practice of the CJEU concerning the interpretation of the legislation and then give a brief overview of what is the current situation. Secondly, the authors focus on Estonian legislation and how the CJEU's decisions and EU legislation have affected Estonian legislation and impacted the perception of the use of communications data as an infringement of fundamental rights. In the third chapter the authors discuss following problems: how long and whose data should be kept by the electronic communications undertakings; the relationship between national security *versus* public security - which needs more data kept by the service providers; is there a need for a new and more specific directive and should over-the-top service providers also retain communication data.

[8] Code of Criminal Procedure. - RT I, 22.12.2021, 45.

I part: The Legal Framework of the European Union and the Case Law of the CJEU

The Charter[9] brings together the most important personal freedoms and rights enjoyed by citizens of the EU into one legally binding document. Concerning data retention, it is important that the legislation is in accordance with Articles 7 and 8 of the Charter. Article 7 states that everyone has the right to respect for his or her private and family life, home and communications. In accordance with Article 8 everyone has the right to the protection of personal data concerning him or her. The second subsection of the article provides that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Charter's Article 52 states that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[10] The Charter therefore reserves the right to restrict rights and freedoms by law, taking into account the nature of the rights and freedoms in accordance with the principle of proportionality.

At European level, Directive 95/46/EC is the reference text on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State sets up an independent national body responsible for the supervision of any activity linked to the processing of personal data. As a general rule, the processing must take place under the conditions referred to Article 6 of the Directive. However, the Directive allows the national legislator to adopt legislation restricting the rights of the data subject provided for on the Directive if this is necessary, for example to safeguard national

[9] Charter of Fundamental Rights of the European Union, OJ 2012 C 326/391.
[10] Charter of Fundamental Rights of the European Union, OJ 2012 C 326/391.

security, defence, public security or to safeguard the prevention, investigation, detection and prosecution of criminal offences.[11]

The development of the market for electronic communications services and technology created the need for additional regulations. Directive 2002/58/EC on Privacy and Electronic Communications, mostly known as the ePrivacy Directive, is the main instrument currently in force on the EU level to protect privacy and it includes specific rules on data protection in the area of telecommunication in public electronic network.[12] Common rules on data retention were introduced in 2006 by Directive 2006/24/EC, which applied to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user for minimum of six months and at the most twenty-four months, in order to allow access by national authorities for the purpose of criminal investigation, detection and prosecution of serious crimes, as defined by each Member State in its national law.[13] According to Article 4 of the Directive 2006/24/EC, it was up to Member States to decide which authorities would have access to the retained data. It was a broader directive that set out a general legal framework, but it was not precise enough to ensure uniform implementation of the directive among the Member States. Some countries did not implement the Directive into national law by the deadline.[14] The reasons were either doubts as to the compatibility of the provisions of the Directive with fundamental rights or decisions of the constitutional courts declaring the laws implementing the Directive unconstitutional, as they unreasonably restricted fundamental rights.[15] The aforementioned Directive was declared invalid by the CJEU in 2014 in its decision *Digital Rights Ireland and Seitlinger*.[16]

The abovementioned decision did not prohibit data retention itself, but the CJEU did assert that the retention of data as provided in the Directive 2006/24/EC violated Articles 7 and 8 of the Charter.[17] More specifically, the Court found that the Directive does not lay down any objective criteria by which the number of persons authorised to access and subsequently use the data

[11] Directive of the European Parliament and of the Council 95/46, OJ 1995 L 281.
[12] Directive of the European Parliament and of the Council 2002/58, OJ 2002 L 201/37.
[13] Directive of the European Parliament and of the Council 2006/24, OJ 2006 L 105/54.
[14] Deadline was on September 15, 2007.
[15] Lõhmus, "Elektroonilise side andmete säilitamise lõpetamata saaga", 10 Juridica (2015).
[16] Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238).
[17] Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238), at para. 69.

retained is limited to what is strictly necessary in the light of the objective pursued.[18] In addition, the CJEU held that the access by the competent national authorities to the data retained should be made dependent on a prior review carried out by a court or by independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued, and the reasoned request to access such data has been submitted in the framework of prevention, detection or criminal prosecutions. The Court also found that the Directive did not lay down any specific obligations on Member States to establish such limits.[19] Even though a number of Member States made amendments to their legislation regarding data retention[20] and some national courts declared national legislation to be invalid[21] on the basis of *Digital Rights Ireland and Seitlinger*, uncertainty still persisted.

The European Commission did not start working on a new directive, but announced in the press release of September 16, 2015 that they would not submit any new proposals to regulate the retention of electronic communications data.[22] Therefore Directives 95/46/EC and 2002/58/EC remained in force and Directive 95/46/EC was repealed in 2016.[23]

Arising from the *Digital Rights Ireland and Seitlinger* case, joined cases submitted by Sweden and the UK were brought upon CJEU to address the issue of compatibility of Swedish and UK national laws on data retention with the Charter. To summarise, the CJEU found in late 2016 in the *Tele2/Watson* case that Swedish and UK national data retention laws exceeded the limits of what is necessary to retain according to the EU legislation. National laws which require the retention of traffic and location data for communications, as well as laws governing access to such data by public authorities, fall within the scope of Directive 2002/58/EC.[24] CJEU also found that the retention of traffic and location data, so that it can be made available to competent

[18] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238), at para. 62.
[19] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (EU:C:2014:238), at para. 62.
[20] e.g. Croatia, Cyprus, Czech Republic, France, Ireland, Poland, Portugal and Spain. - Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment* (2017), available at https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf , at 12.
[21] e.g. Slovakia, Slovenia, Romania, Austria, Bulgaria, Belgium and Netherlands. - Lõhmus, "Elektroonilise side andmete säilitamise lõpetamata saaga", 10 Juridica (2015), at 740.
[22] Commission Statement of 16 September 2015, OJ 2015 L15/5654.
[23] Regulation of the European Parliament and of the Council 2016/679, OJ 2016 L 119/1.
[24] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige/Watson* (EU:C:2016:970), at para. 73, 76.

authorities if necessary, infringes extensively and severely a number of fundamental rights.[25] CJEU found that Article 15 of Directive 2002/58/ EC, in the light of Articles 7, 8, 11 and 52 (1) of the Charter, must be interpreted in a way that national legislation which for the purposes of combating crime, imposes an obligation on retaining all electronic communications in a general manner and without any distinction of all traffic and location data of all subscribers and registered users, is not in accordance with EU law. Court also found that the aforementioned articles also precluded national rules governing the protection and security of traffic and location data and, in particular, access to retained data by the competent authorities, without restricting that access to the fight against serious crime, without making access to the data subject to prior judicial or independent administrative review, and without requiring that the data be stored in the territory of the EU. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in some particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.[26]

The next significant decision was *La Quadrature du Net*[27] in which CJEU did not change its position regarding communication data retention - the general and indiscriminate retention of all traffic and location data of all users disproportionately violates the fundamental rights provided by Articles 7, 8 and 11 of the Charter.[28] Instead, CJEU proposed targeted data collection and storage - such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime.[29]

---

[25] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige/Watson* (EU:C:2016:970), at para. 100.
[26] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige/Watson* (EU:C:2016:970), at para. 119, 134.
[27] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* (EU:C:2020:791).
[28] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* (EU:C:2020:791) at para. 111.
[29] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* (EU:C:2020:791), at para. 144.

However, following these significant judgments, the Member States continued with their previous approach and no substantive change took place. The interpretation of judgements also differs from one Member State to another. To cite the Republic of Estonia as an example, there are differences of opinions that have become a matter of concern over time, which will be discussed in more detail in the next section.

II part: Use of Communication Data and its Retention in Estonia

Until 1 January 2013, the article 117 of the Estonian Code of Criminal Procedure (hereinafter CCP)[30] provided that the collection of data on messages transmitted over public technical communication channels[31] was a surveillance activity which could be conducted with a permission of the prosecutor in charge of the proceedings. Requesting communication data as a surveillance activity allowed several control and supervision bodies to monitor that surveillance activities comply with the law. This is due to the fact that in Estonia surveillance activities are considered a state secret.

After 1 January 2013, amendments to the law were made and since then requesting communication data was no longer surveillance activity, but instead a "regular procedural operation", which was no different from habitual address or real estate inquiry. Though legislator confirmed[32] that control over data requests is still in place, it was not possible to ensure the former control over data requests. The right to give permission to the investigative body to request communication data from operators of the electronic communication network was given to the Prosecutor's Office under the clause that the request may be made only if "*it is strictly necessary for the purpose of the criminal proceeding*" (the so-called *ultima ratio* principle). It is worth mentioning that CCP Article 213 states that the Prosecutors' Office shall direct pre-court proceedings. This meant that giving the permission to the investigative body was not dependent on a prior review carried out by a court or by an independent administrative body.

[30] Code of Criminal Procedure - RT I, 17.04.2012, 6.
[31] Section 117 of Estonian CCP provided that data was collected from the operator of the electronic communication network in order to determine the fact, duration, manner and form of transmission and the personal data and location of the transmitter or recipient.
[32] The explanatory memorandum to a draft of Code of Criminal Procedure, 18 January 2012, available at: https://eelnoud.valitsus.ee/main#b4KHlU4B.

When in 2014 CJEU declared the Directive 2006/24/EC invalid, Estonian legislator did not amend the law in any way. Since 2008 the Article 111[1] subsection 4 of the Electronic Communications Act[33] (hereinafter ECA) has provided that communication data is retained for one year from the date of the communication without distinguishing between the people whose data is stored.

The question of whether the laws in force contradict the views of the CJEU first arose in the Supreme Court of Estonia judgment 3-1-1-51-14. [34] In the case, three persons were accused of committing a criminal offence qualified pursuant to subsection 1 of § 212 of the Penal Code of Estonia[35] (insurance fraud). One of the accused's counsel argued that the communication data used as evidence was inadmissible, because the data had been stored unlawfully in the criminal proceedings based on a judgement of the Court of Justice of the European Union *Digital Rights Ireland and Seitlinger*.

Although lawyers, legal experts[36] and two members of the Criminal Chamber of the Court disagreed, the Supreme Court of Estonia found that the invalidity of the Directive 2006/24/EC does not necessarily lead to the invalidity of national regulations and assessment of the case should be given after specific regulatory control. Court found that the measure is appropriate and facilitates the capture of criminals. Data retention for one year from the date of the communication was not an excessive amount of time and the evidence was admissible.

The Chancellor of Justice also attended the issue of the constitutionality of the data retention and further processing of electronic communications data stipulated in § 111[1] of the ECA[37] after the

---

[33] Electronic Communications Act. - RT I, 27.02.2022, 3.
[34] Supreme Court of Estonia 3-1-1-51-14.
[35] Penal Code. - RT I, 21.05.2021, 9.
[36] e.g. Lõhmus, "Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte", 10 Juridica (2016).
[37] Chancellor of Justice, *Opinion of the Chancellor of Justice about the constitutionality of § 111[1] of the Electronic Communications Act*, 20 July 2015, available at: https://www.oiguskantsler.ee/sites/default/files/field_document2/Constitutionality%20of%20the%20retention%20and%20further%20processing%20of%20electronic%20communications%20data%20stipulated%20in%20%C2%A7%20111%20prim%201%20of%20the%20Electronic%20Communications%20Act.pdf.

Directive 2006/24/EC was declared invalid.[38] The Chancellor of Justice only assessed the constitutionality of the communications data processing in the part that concerns the collection and retention of data by the communications operators, leaving out requesting communications data by public authorities. The Chancellor of Justice concluded that the collection and further processing of personal data infringes § 26 of the Constitution of the Republic of Estonia ("*everyone has the right to the inviolability of private and family life*")[39]. Since ECA § 111[1] does not prescribe the collection and further processing of data that concerns the content of the messages transmitted in electronic information channels, the Chancellor of Justice found that it is impossible to refer to any specific measures that would clearly be as effective in the light of the protection of public order. Assessing the moderateness of the interference, the continuing increase in the share of electronic communications and the need to combat serious crime effectively outweighs the intensity of the infringement which is caused by the fact that data is automatically collected and retained, and prescribed for all generally used means of communication in the Chancellor's opinion. In addition, the Chancellor of Justice found that it is unclear how and based on what criteria it would be possible to retain communications data selectively.[40] This ambiguity is still a problem today and is further discussed in the third section of the paper.

From the time the CJEU decision *Digital Rights Ireland and Seitlinger* was made until 2022, the situation in Estonia regarding data retention and requesting communications data by public authorities and investigative bodies was unclear. The problems were mainly related to the

[38] *Electronic Communications Act § 111[1] subsection 2: The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:*
1) the number of the caller and the subscriber's name and address;
2) the number of the recipient and the subscriber's name and address;
3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;
4) the date and time of the beginning and end of the call;
5) the telephone or mobile telephone service used;
6) the international mobile subscriber identity (IMSI) of the caller and the recipient;
7) the international mobile equipment identity (IMEI) of the caller and the recipient;
8) the cell ID at the time of setting up the call;
9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;
10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

[39] The Constitution of the Republic of Estonia. - RT 1992, 26, 349.

[40] Chancellor of Justice, *supra* note 37, at 7.

definition of what is a serious crime, whether and whose data to retain and for how long, and should there be a prior review by the court or an independent administrative authority to control the access of the competent national authorities to retained data.[41]

The problem of retaining and accessing communication data was not an easy task for the legislator to solve. Regardless of several decisions of the CJEU, the consequences of the conditions imposed by the Court were unclear in terms of legal and practical applicability. This led to a situation where the Supreme Court of Estonia asked the CJEU for a preliminary ruling on November 12, 2018.[42]

In the aforementioned case[43], H. K. was accused of larceny, computer-related fraud and violence against a person participating in administration of justice. Communication data protocols received from the providers of electronic communications services, were used as evidence in the case. H. K.'s counsel challenged the decisions of lower courts, arguing that protocols received from the providers of electronic communications service are not admissible evidence and should be dismissed, since Estonian legislation that requires electronic communication service providers to retain communication data, as well as the use of such data, is in conflict with Article 2 of Directive 2002/58/EC. These arguments led to the situation where the Supreme Court of Estonia suspended the proceedings and asked three questions from the CJEU.[44] With its first and second questions, the court asked, in essence, whether Article 15(1) of 2002/58/EC, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of communication data to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime, regardless of the length of the period in respect of which access to those data is sought and the quantity and the nature of the data available in respect of such a period. With its third question, the Court asked, whether

---

[41] Lauri (Minister of Justice of Estonia), *Sideandmetest nii ja naa*, 24 September 2021. Available at: https://www.err.ee/1608349664/maris-lauri-sideandmetest-nii-ja-naa.
[42] 12 November 2018 Supreme Court of Estonia 1-16-6179.
[43] Also known as dog sausage case, because the object of the larceny was not only money and food but also dog sausage.
[44] Case C-746/18, *H.K. v Prokuratuur* (EU:C:2021:152), at para. 26.

Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public Prosecutor's Office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

In conclusion, the CJEU found in the case C-746/18 *H. K. vs Prokuratuur* that Article 15 (1) of Directive 2002/58/EC, read in the light of Articles 7, 8, 11 and Article 52 (1) of the Charter, must be interpreted as "*precluding national legislation that permits public authorities to have access to a set of location data*[45] *.... for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period*." CJEU also found that prosecutors do not have the power to authorise access of a public authority to communication data for the purposes of a criminal investigation.

CJEU sent a clear message that Estonian law does not guarantee a fair balance between the prevention, investigation and prosecution of criminal offences in the field of electronic communications and access to location data and the right to privacy, protection of personal data and freedom of expression[46], due to which the use of communication data in criminal proceedings in Estonia became impossible. On June 18, 2021 Supreme Court of Estonia found that authorization to use and use of unlawfully stored data is prohibited following the *La Quadrature du Net* decision and the retention of personal data is contrary to Article 15 (1) of Directive 2002/58/EC. The court ruled that from 7 October 2020, a breach of privacy through the use of unlawfully stored data must be considered intentional and serious and entails a ban on the

[45] "*...that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life…"*

[46] Lõhmus, "Elektroonilise side metaandmete säilitamise ja kasutamise saaga uued peatükid", 3 Juridica (2021), at 167.

use of the data obtained as evidence in criminal proceedings.[47] However, such position did not come as a surprise to any lawyer who was familiar with the subject.[48]

As it was no longer possible to ask for communications data with the permission of the public prosecutor and the law was not amended quickly, the Prosecutor's Office tried to approach the problem creatively. The Prosecutor's Office tried to obtain communications data by submitting a search request to the court - a "search" was conducted on the servers of providers of electronic communications services and the object of the search was communication data on digital documents. This way it was possible to have a prior review of the request by the court.

About half a year after the preliminary ruling of the CJEU, the Estonian legislator amended the CCP. Purpose of the amendment was to be in compliance with Directive 2002/58/EC, taking into account CJEU's orders in the decision C-746/18.[49] CCP now provides that an application of the Prosecutor's Office needs an authorisation from the pre-trial investigation judge in the pre-trial proceedings to make an enquiry to an electronic communications undertaking concerning data that is listed in subsections 2 and 3 of § 111^1 of the ECA.[50] The law was also supplemented with a condition that an enquiry may be made if the criminal offence[51] is one listed in the subsection 2 of § 126^2 of the CCP.

Despite the fact that the law now provides a list of offences for which it is justified to require an electronic communications undertaking to provide data, it is still a question of whether the offences mentioned in the list are serious enough to justify a widespread violation of fundamental rights. Also, the legislator has not yet amended the subsection 4 of § 111^1 of the ECA, which provides that communication data of all persons shall be preserved for one year from the date of the communication thus still contradicting the views of the CJEU.

---

[47] 18 June 2021 Supreme Court of Estonia 1-16-6179, at para. 106.
[48] *E.g.* Schasmin and Ginter, "Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis", 1 Juridica (2017).
[49] The explanatory memorandum to a draft of Code of Criminal Procedure, 18 January 2012, available at: https://eelnoud.valitsus.ee/main#b4KHlU4B.
[50] Code of Criminal Procedure. - RT I, 22.12.2021, 45.
[51] Subsection 2 of § 126^2 of CCP of Estonia lists the criminal offences for which surveillance activities may be conducted - among Estonian lawyers, those are often referred to as "catalogue crimes".

III part: The Authors' Suggestions for Mitigating the Situation

3.1. Whose Data Should be Retained by Communications Service Providers?

Already in the decision C-293/12 *Digital Rights Ireland and Seitlinger*, the CJEU has ruled that it is problematic to store the communication data of all individuals by providers of electronic communications services, whether or not public authorities need access to the data. However, CJEU did not specify in the decision whose data should be retained and whose data should not.

CJEU examined the above question[52] in more detail in decision *La Quadrature du Net*[53]. CJEU found, in essence, that only the fight against serious crimes and the prevention of a serious threat to national security justify serious infringements of a fundamental right in accordance with the principle of proportionality. Data retention cannot be the rule but the exception. Data retention is generally allowed in the interests of national security, but CJEU found that in the interests of public security, data should be collected and retained if they meet certain criteria - (a) data for a specific period of time and / or (b) data for a specific geographical area and / or (c) data on persons who may be involved in a serious crime, or (d) data on persons whose data retention can contribute to the fight against serious crime.[54]

However, the above distinction is in stark contrast to Article 21 of the Charter, which prohibits any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. In particular, the question arises when, for example, the data of persons living in a high-crime area are retained - the high-crime area is also likely to be home to law-abiding people whose fundamental rights would be unduly violated by such data retention. It must be concluded from the above that it is not possible to determine whose data is to be retained on the basis of the criteria laid down by the CJEU.

---

[52] Whether Article 15(1) of Directive 2002/58 must be interpreted as precluding national legislation which imposes on providers of electronic communications services, for the purposes set out in Article 15(1), an obligation requiring the general and indiscriminate retention of traffic and location data

[53] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* (EU:C:2020:791).

[54] Lõhmus, *supra* note 46, at 171.

It is certainly more likely that those previously convicted of a criminal offence are involved in serious crime than those who have not been previously convicted. However, serious crimes are often also committed by those who have not previously been convicted. Retaining only the data of persons who have previously been convicted of a criminal offence is likely to lead to a situation where communication between criminals takes place using numbers of law-abiding persons, which in turn renders the use of communications data meaningless in such criminal proceedings. In essence, the CJEU has ruled that the rights of victims must also be taken into account in its deliberations, but has made the retention of data subject to certain criteria which render victims' rights meaningless.

The Estonian legislator has not yet made any amendments to the law that would allow a communication service provider to distinguish whose data is stored and whose data is not. Subsection 4 of § 111^1 of the ECA provides that communication data of all persons shall be preserved for one year from the date of the communication. The Estonian legislature has probably not made any changes as the situation is still incomprehensible. Maintaining only the communication data of selected individuals can leave many criminal cases unresolved - with no compensation for victims of crime.

The authors of the present work consider that the violation of fundamental rights in the retention of data is significant, but due to Article 6 of Directive 2002/58/EC traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. Due to the above - if traffic data is allowed to be retained by communication service providers, why not retain other communications data under the following conditions.

1. Communication service providers retain all communication data for a short period of time (e.g. maximum one year). In that case, there would be no conflict with Article 21 of the Charter. The European legislator could regulate more strictly the use of data by communication service providers, so that service providers only use data to the extent necessary - to the extent that it does not allow the service provider to draw accurate conclusions about a person's private life. If the data of all persons is retained, while at the

same time laying down strict rules on access to data by public authorities, public authorities will not be able to draw indiscriminate inferences about a person's private life.

2. The authors agree with the CJEU that access should be a subject to prior review by a court or an independent administrative authority. Asking the court for access significantly increases the court's workload, but prevents unjustified inquiries into the communication service provider. However, the authors consider that requesting access to communications data from a court should only take place if collection of data by other activities or taking of evidence by other procedural operations is impossible, is impossible on time or is especially complicated or if this may prejudice criminal proceedings in the case.[55] The court should check whether this is a last resort to resolve the criminal case or whether other procedural operations can be taken to identify the offender. However, prior judicial review can be a major problem in smaller Member States (e.g. Estonia), as the European Convention on Human Rights[56] puts pressure on fast-track criminal cases. In connection with additional tasks to the court it can interfere with everyone's right to a hearing within a reasonable time. On the other hand - taking control of requests for communications data from the court leads to a situation where there is basically no control over the request for communications data in criminal matters. E.g, in 2021, 4387 out of 4704 criminal cases were resolved by simplified procedures in Estonian county courts.[57] This means that only 317 criminal cases, which were settled in general proceedings[58], were subject to subsequent control over the requests for communications data. In conclusion, prior judicial review is necessary to prevent violations of the fundamental rights of individuals and partial subsequent review is not sufficient to ensure the correct application of EU law by courts of the Member States.
3. The request and use of communications data in the above form should be permitted where national law provides for the right to judicial remedy in the event of a breach of rights in the processing of the data. This obligation on Member States to provide judicial

---

[55] *Ultima Ratio* principle - also provided in subsection 2 of § 126[1] of CCP of Estonia, which governs surveillance activities.

[56] European Convention on Human Rights Article 6.

[57] Kohtute menetlusstatistika (2021), available at: https://www.kohus.ee/dokumendid-ja-vormid/kohtute-menetlusstatistika.

[58] In general proceedings the court will assess whether communication data received from communication data undertakings is admissible evidence.

remedies to individuals is already set out in general terms in European Union Directive 95/46/EC.

Also the problem of distinguishing between public and national security is noteworthy. CJEU found in decision *La Quadrature du Net*, that it is important to distinguish national security from public security - the court found that more serious violations of fundamental rights were justified in the light of the objective of protection of national security than in the case of the other objectives mentioned in the Article 15(1) of Directive 2002/58/EC. In essence CJEU found that in the interests of national security, general and indiscriminate data retention was permitted, if a time limit is set. In the case of public security, a clear distinction must be made between those whose data are to be retained.[59] However, if the authors' above conditions for data retention are met, the problem of distinguishing between national and public security will not arise either. It is impossible to determine whose data will be retained in the interests of national security.

As mentioned above, the issue of communication data retention remains an issue, as long as there is no directive or court decision that unambiguously and clearly regulates or interprets the situation. This raises the question of whether the European legislator should nevertheless step back from the previous position[60] and regulate the sector.

3.2. Data retention in the light of the possible new ePrivacy Directive and over-the-top service providers

The role of the internet in our society is constantly growing - which in turn means that broadband cellular technologies are also evolving extremely fast.[61] Even nowadays a very large proportion of calls and messaging take place over the internet in different apps on social media platforms (i.e it's possible to make calls on Facebook Messenger, WhatsApp, Telegram, Signal over internet broadband). However, these technological innovations mean that data retention in its traditional sense is losing its relevance.[62] In Estonian ECA the electronic communications

[59] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* (EU:C:2020:791), at para. 138.
[60] Commission Statement of 16 September 2015, OJ 2015 L15/5654.
[61] 5G in Estonia, available at: https://5geestis.ee/.
[62] Virks, *supra* note 6, at 584.

undertaking is defined as "*a person who provides publicly available electronic communications services to the end-user or to another provider of publicly available electronic communications services*" - by this definition social media platforms don't fall under its scope and thus do not have a legal obligation to retain communication data. This means that over-the-top (hereinafter OTT) service providers, i.e. companies operating on the internet without operator intervention, do not currently have the legal obligation to retain communications data.[63]

Since January 2017 there have been talks and possible proposals for a new ePrivacy Regulation - it is an update of the EU ePrivacy Directive 2002/58/EC which was revised in 2009. The Digital Single Market Strategy (hereinafter DSM Strategy) has as an objective to increase trust in the security of digital services. The reform of the data protection framework, and in particular the adoption of Regulation (EU) 2016/679, the General Data Protection Regulation (hereinafter GDPR), was the key action to this end. The DSM Strategy also announced the review of the ePrivacy Directive in order to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. The new ePrivacy Regulation proposal reviews the ePrivacy Directive, foreseeing the DSM Strategy objectives and ensuring consistency with the GDPR.[64]

The ePrivacy Regulation is self-executing and becomes legally binding across the EU. This would be a common solution and would not create as much confusion in the Member States as the implementation of the directive did. It is proposed that the new regulation should also include in its scope undertakings that use OTT services, with the aim of ensuring a level playing field for companies.[65] As of March 2022, the aforementioned proposal has not much moved forward, which means that the impact of the new regulation on the retention of communications data, including data retention obligation on OTTs, is still an open question. At the moment in criminal proceedings conducted in Estonia the only possible way to get information from OTTs is through regular procedural operations (submitting an inquiry to the OTT by the body conducting the

[63] Virks, *supra* note 6, at 584.
[64] Proposal for the Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communication) COM/2017/010 final-2017/03 (COD).
[65] Legislative Train Schedule, *Proposal for a Regulation on Privacy and Electronic Communications* (2022), available at: https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform.

proceeding). As the asked data is usually handled outside of Estonian territory (and often outside of EU's territory as well), this would mean using international cooperation, where getting an answer within reasonable time frames is often unachievable. Thus, if OTTs were to be also included in the new ePrivacy Regulation, this would guarantee more uniform legislation regarding data collected (including the data collected by OTTs) and used within all Member States. More precise regulation that includes OTTs in addition to electronic communication operators would ensure that regardless of the way the communication takes place, the rules regarding collecting and using such data are harmonised across Member States.

Conclusion

The retention of communication data has been the subject of most data related discussions since Directive 2006/24/EC was adopted by the European Parliament and Council of Europe. The aforementioned Directive was repealed in 2014 by the CJEU in its landmark decision *Digital Rights Ireland and Seitlinger*. CJEU found that the Directive 2006/24/EC covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime, and such retention of data does not comply with the Directive. However, legal uncertainty in European Union Member States' legislation is still present to this day.

The authors in this paper gave an overview of Estonian legal regulation concerning data retention. When in 2014 the Directive 2006/24/EC was declared invalid, Estonian legislator did not amend the law in any way. Although it was noted amongst local legal scholars that the Estonian legislation very likely infringes EU law, the Supreme Court of Estonia found that the invalidity of the Directive 2006/24/EC does not necessarily lead to the invalidity of national regulations. The Chancellor of Justice found in 2015 that it is impossible to refer to any specific measures that would clearly be as effective in the light of the protection of public order as the retention of communication data. As uncertainty persisted the Supreme Court of Estonia asked the CJEU for a preliminary ruling on November 12, 2018. However, the CJEU ruling in the case *H. K. vs Prokuratuur* sent a clear message that Estonian law does not guarantee a fair balance between the prevention, investigation and prosecution of criminal offences in the field of electronic communications and access to location data and the right to privacy, protection of personal data and freedom of expression. Since the ruling there have been amendments made to the Estonian law.

The saga concerning the retention of communication data has yet to come to an end in the EU. The authors acknowledge that finding a suitable solution in the retention of communication data is not an easy task for European legislators to solve. Though in the third part of this paper, the authors discussed further possible problems and their solutions, one thing is crystal clear: finding a balance between individuals' right to demand a protection of one's fundamental rights from the

state and the right to demand for the state not to intervene with their private lives has proved to be a challenging task. The authors of this paper set out their vision of current possible problems and solutions and hope that a suitable resolution will be found within the EU that both guarantees people their privacy, but at the same time allows the fight against serious crime to continue effectively.