



Revista  
Brasileira de  
**Direito**  
**Processual**  
**Penal**

Volume 7 - Nº 01 - jan./abr. 2021

ISSN 2525-510X

<https://doi.org/10.22197/rbdpp.v7i1>

**Dossiê**

*“Admissibilidade da prova no processo penal: entre a busca pela verdade, os direitos humanos e a eficiência do procedimento”*




IBRASPP

# Collection of location data in criminal proceedings – European (the EU and Strasbourg) standards

*Coleta de dados de localização no processo penal – Parâmetros europeus (EU e Strasbourg)<sup>1</sup>*

**Dominika Czerniak<sup>2</sup>**

University of Wrocław, Poland  
dominika.czerniak@uwr.edu.pl

 <https://orcid.org/0000-0002-8970-4017>

---

**ABSTRACT:** This article deals with the problem of collecting, retaining and processing location data for use in criminal proceedings. The collection of location data is an interference with the right to privacy (the Article 8 of the ECHR, the Article 7 of the Charter). However, such interference is permissible if it pursues the aims indicated in Article 8(2) of the ECHR (prevention of and fight against serious crime, protection of general security, national security). Therefore, the question arises as to when the procedural authorities may obtain location data (what offences may justify interference with the right to privacy) and what conditions should be met by national law with regard to this issue. The ECtHR and the CJEU are increasingly dealing with cases that concern the collection of location data in real time and data retention by telecommunications service providers. This requires an assessment of whether a European standard has now been developed and, if so, what is the standard?

**KEYWORDS:** Criminal procedure; Human rights; Right to privacy; Location data; Data retention.

**RESUMO:** *Este artigo analisa o problema da coleta, custódia e processamento de dados de localização para uso em processos penais. A coleta de dados de*

---

<sup>1</sup> This work is a result of the research project funded by the National Science Centre No. 2017/27/B/HS5/00854

<sup>2</sup> PhD candidate, University of Wrocław, Poland.

*localização é uma restrição ao direito à privacidade (art. 8, CEDH; art. 8, Carta de Direitos Fundamentais da UE). Contudo, isso é permitido se almejar o objetivo indicado no art. 8(2) da CEDH (prevenção e combate a crimes graves, proteção da segurança pública e nacional). Assim, a questão surge sobre quando as autoridades podem obter os dados de localização (quais crimes podem justificar essa restrição à privacidade) e em que condições devem ser respeitadas pelas legislações nacionais sobre o tema. O TEDH e o Tribunal de Justiça da UE estão lidando cada vez mais com casos relacionados à coleta de dados de localização em tempo real e a sua custódia pelos provedores de serviços de telecomunicações. Isso a verificação de se os parâmetros europeus foram desenvolvidos e, em caso positivo, quais são eles.*

**PALAVRAS-CHAVE:** processo penal; direitos humanos; direito à privacidade; dados de localização; custódia de dados.

---

## 1. INTRODUCTION

Location data allows determination of the profile and routine of life, the place where one stays and for how long one stays in a given place<sup>3</sup>. The collection, processing and storage of such data is an interference in the right to privacy (Article 8 of the ECHR<sup>4</sup>, Articles 7 and 8 of the Charter<sup>5</sup>). Constant monitoring of an individual's behaviour, wherever they are, may give the impression that he/she is under constant surveillance. There is no doubt, however, that location data can provide relevant information that can assist authorities involved in criminal proceedings. Intervention into the sphere of privacy of an individual is warranted as long as it serves the purposes indicated in art.

<sup>3</sup> STACHNIK-ROGALSKA, Agnieszka; ROGALSKI Maciej. Udostępnianie billingów rozmów telefonicznych. *Państwo i Prawo* no. 8, p. 31-32, 2012.

<sup>4</sup> EUROPEAN CONVENTION OF HUMAN RIGHTS, adopted in Rome on 4<sup>th</sup> November 1950. Available at: [https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf). (access: December 20, 2020). Hereinafter: the ECHR.

<sup>5</sup> CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, published in the Official Journal of the European Union no. C 326/391 on 26<sup>th</sup> October 2012. Available at: <https://eur-lex.europa.eu/legal-content/EN/TX-T/?uri=CELEX:12012P/TXT>. Hereinafter: the Charter.

8 sec. 2 of the ECHR, and the interference itself fulfils the condition of proportionality and necessity in a democratic society<sup>6</sup>. The restriction of the rights of an individual must be proportionate to the aims that the procedural organs wish to achieve, and the expected positive consequences (ensuring public safety, combating crime) must exceed the negative consequences of violating rights and individual freedom.

In EU law, as defined in Directive 2002/58/EC and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter: Directive on privacy and electronic communications; Directive 2002/58) “location data” is understood as “any data processed in an electronic communications network, indicating the geographical location of the terminal equipment of a user of a publicly available electronic communications service”<sup>7</sup>. They are considered a type of “personal data”<sup>8</sup> within the meaning of Directive 2016/680 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of crime prevention, investigation, detection and prosecution of offences and execution of punishments, on the free movement of such data and repealing Council Framework Decision 2008/977 / JHA (hereinafter: Directive 2016/680)<sup>9</sup>. The Strasbourg Court<sup>10</sup> - in view of the absence of a separate definition of location data in legal acts adopted at the

---

<sup>6</sup> BREYER, Patric. Telecommunication Data Retention. *European Law Journal*, v. 11, no. 3, s. 365, 2005.

<sup>7</sup> The Official Journal of the European Union no. L 201/37 on 31<sup>st</sup> July 2002. See: article 2 point c.

<sup>8</sup> In accordance with the Article 3 of the Directive 2016/680 “personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

<sup>9</sup> The Official Journal of the European Union no. L 119/89 on 47<sup>t</sup> April 2016.

<sup>10</sup> The European Court of Human Rights.

forum of the Council of Europe - uses the definitions adopted in the European Union<sup>11</sup>.

The CJEU<sup>12</sup> and the ECtHR<sup>13</sup> emphasise the need to balance the interests of the individual and the protection of public safety<sup>14</sup>. The rights to privacy and confidentiality of location data are an important value in a democratic society, but in justified cases, e.g. in connection with the need to fight and prevent crime, it is permissible to interfere with the rights of an individual. Based on the case law of the European Courts and current legislation, it is possible to establish rules for the collection of location data in national law for the purpose of using this data in criminal proceedings. Before analysing this issue, however, it should be clarified how the procedural authorities can obtain location data. Following the ECtHR jurisprudence<sup>15</sup>, the following can be distinguished:

- 1) real-time data collection (e.g. using GPS transmitters), and
- 2) obtaining “historical” data, i.e. retained by telecommunications service providers (e.g. from radio transmitters) or collected by applications installed on smartphones and saved on these devices (e.g. data on places where one connects to the wifi network, data derived from Google maps).

As for the technical aspects of locating, for example a smartphone user, it is possible to indicate systems based on: 1) obtaining location data based on GPS; 2) connecting the smartphone to the wi-fi network; 3) GSM technology; 4) determining the location of the radio signal; 5) GNSS.<sup>16</sup> The technical aspects of collecting and obtaining location data - although important for smartphone users, tablets, etc. - are of little

<sup>11</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, Ben Faiza v France, case no. 31446/12. <https://hudoc.echr.coe.int/>.

<sup>12</sup> The Court of Justice of the European Union.

<sup>13</sup> The European Court of Human Rights.

<sup>14</sup> DOCKSEY, Christopher, HIJMANS, Hielke, The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law. *European Data Protection Law Review* (EDPL), vol. 5, no. 3, p. 300-316, 2019.

<sup>15</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, Ben Faiza v France, case no. 31446/12. <https://hudoc.echr.coe.int/>.

<sup>16</sup> BU-PASHA, Shakila, ALEN-SAVIKKO, Anette, MEIKINEN, Jenna, GUINNESS, Robert, KORPISAAR, Päivi. EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency. *European Data Protection*

importance from the perspective of establishing the rules for accessing this data. Whatever the information gathering technique, access can only be obtained in two ways - either in real time or ex post.

Interference in the privacy of individuals cannot be arbitrary - state authorities cannot 'cut corners' to ensure security and public order. Although the technical possibilities for tracking an individual's behaviour are almost unlimited, they should not be overused. The aim of this paper is to determine whether there is a common European standard for the gathering and processing of location data to prevent and combat crime. The ECtHR and the CJEU are increasingly addressing this issue. However, the question arises whether, at this stage, it is reasonable to claim that a standard has already emerged.

The jurisprudence of the ECtHR and the CJEU is structured according to the way in which data is collected, i.e. either in real time or ex post (from mobile phone companies). The decisions of the Strasbourg and Luxembourg tribunals were analysed chronologically. This method made it possible to show the evolution of the case law and the attempt to adapt the rulings to changing technical conditions.

## 2. LIMITATION OF THE RIGHT TO PRIVACY – GENERAL RULES

The collection of location data in the case-law of the ECtHR is considered under Art. 8 of the ECHR. In assessing a complaint of a breach of the right to privacy, the Court takes into account three factors<sup>17</sup>:

1. the existence of legal bases in domestic law allowing interference in the sphere of privacy of an individual;

---

*Law Review (EDPL)*, vol. 2, no. 3, p. 312-323, 2016. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=57&id=&page=>

<sup>17</sup> See also: GARLICKI, Lech in: GARLICKI, Lech, HOFMAŃSKI, Piotr. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa 2011; JASIŃSKI, Wojciech, *The limits of interference with the right to liberty, privacy property and privilege against self-incrimination in criminal proceedings – European standards*, in: SKORUPKA, Jerzy (ed.), *The Model of Acceptable Interference with the Rights and Freedoms of a Individual in the Criminal Process*, p. 450; 463. Warsaw 2017.

2. the implementation by public authorities of the objectives indicated in Art. 8 sec. 2 of the ECHR

3. the necessity to interfere with the right to privacy in a democratic society<sup>18</sup>.

The requirement that any interference with the individual's right to privacy be properly grounded in national legislation is tied to the necessity of ensuring the predictability of the procedure. In the judgement in the case Roman Zakharov against Russia, the Court recalled that the predictability of the proceedings does not mean that a given person should be able to predict when discreet surveillance measures will be imposed on him and therefore be able to adapt his behaviour to the situation<sup>19</sup>. The point is, however, to define the limits of the legality of the actions of public authorities, in order to prevent arbitrary interference with the privacy of an individual. The minimum guarantees that should be provided are:

1. determination of the nature of crimes in cases for which covert surveillance measures may be applied, but the catalogue cannot be too wide;

2. defining the categories of persons against whom covert surveillance measures may be taken;

3. setting a time limit for the application of these measures;

4. establishing a procedure for testing, using and storing data;

5. introducing precautionary measures when communicating data to other people;

6. specifying the circumstances when data may be deleted or destroyed<sup>20</sup>.

The ECtHR also points to the necessity of finding an appropriate balance between the interests of the state and the pursuit of public security

---

<sup>18</sup> JASIŃSKI, Wojciech, The limits of interference with the right to liberty, privacy property and privilege against self-incrimination in criminal proceedings – European standards, in: SKORUPKA, Jerzy (ed.), *The Model of Acceptable Interference with the Rights and Freedoms of a Individual in the Criminal Process*, p. 450, Warsaw 2017.

<sup>19</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 4 December 2015*, Roman Zakharov v Russia, case no. 47143/06, § 229. <https://hudoc.echr.coe.int/>.

<sup>20</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 4 December 2015*, Roman Zakharov v Russia, case no. 47143/06, § 231. <https://hudoc.echr.coe.int/>.

(and achievement of the objectives of Article 8 (2) of the ECHR). The margin of freedom of states in introducing specific normative solutions is limited and subject to “supervision” of the Tribunal in Strasbourg<sup>21</sup>. Technical measures aimed at protecting a democratic society must not lead to the destruction of democracy in a given country. When interpreting the concept of “necessity”, the Court indicates that it should be understood as a situation in which the interference is justified by a pressing social need, proportionate to the legitimate aim pursued<sup>22</sup>. Therefore, it is crucial to put in place effective and adequate procedural guarantees to prevent possible abuses. The nature and type of procedural guarantees depend on the degree of interference with the privacy of the individual. The more intrusive the activity is, the stronger these guarantees should be provided for the individual.

### **3. REAL-TIME DATA COLLECTION**

#### **3.1. REAL-TIME DATA COLLECTION IN THE ECtHR JURISPRUDENCE**

The first case in which the Strasbourg Court analysed problematic real-time data collection was the case of *Uzun vs. Germany*<sup>23</sup>. The applicant - suspected of participating in a terrorist group and committing crimes in connection with the activities of that organisation<sup>24</sup> - was ordered to be under secret surveillance and tracked via a GPS transmitter in his car. Thanks to the information obtained from real-time location data collection, the trial authorities obtained incriminating evidence, which then became the basis for his conviction. Although the applicant was not

---

<sup>21</sup> See also: STEIN Shlomit, In Search of ‘Red Lines’ in the Jurisprudence of the ECtHR on Fair Trial Rights. *Israel Law Review* v. 50, no. 2, p. 177–209, 2017.

<sup>22</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, *Uzun v Germany*, case no. 35623/05, § 78-79. <https://hudoc.echr.coe.int/>.

<sup>23</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, *Uzun v Germany*, case no. 35623/05. <https://hudoc.echr.coe.int/>.

<sup>24</sup> An organization was called “Antiimperialistische Zelle”. The applicant was convicted for attempted murder and causing four explosion (terrorist attack) to 13 years imprisonment. EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, *Uzun v Germany*, case no. 35623/05, § 11, 17 and 49.



personally subject to geolocation - a GPS transmitter was installed in the car and therefore the movements of every person who used the vehicle were monitored<sup>25</sup> - the ECtHR found that the measures applied constituted an interference with the right to privacy (Article 8 of the ECHR)<sup>26</sup>. However, the Strasbourg Court noted that the collection of location data should be distinguished from that of surveillance, which is video or sound recording. By their very nature, covert surveillance methods that permit “spying” on a person’s life are more intrusive to privacy than GPS data observation and collection. Assessing the provisions of the German Code of Criminal Procedure<sup>27</sup> from the perspective of “lawfulness” and predictability of the proceedings, the ECtHR noted that they did not refer directly to the possibility of applying geolocation surveillance, but indicated the possibility of using technical means - other than image or sound recording - enabling the determination of the observed person’s whereabouts. Sharing the position of the German courts, the ECtHR decided that in connection with the development of technology in the field of Art. 100c § 1 section 1 lit. b of the German Code of Criminal Procedure it also included collecting location data using a GPS transmitter. Although at that time there were no regulations limiting the duration of geolocation surveillance, the regulations required that one month from the date of ordering surveillance by the prosecutor, the observation was extended by the court<sup>28</sup>. Judicial control was an important guarantee against the use of illegally obtained location data and the arbitrariness of the actions of law enforcement agencies. In the opinion of the ECtHR - and due to the fact that geolocation surveillance interferes less with the sphere of privacy of an individual than, for example, control and recording

---

<sup>25</sup> It is worth to mention that the car, where the GPS transmitter was installed by the public authorities, did not belong to the applicant, but to his partner. EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, Uzun v Germany, case no. 35623/05, § 11, 17 and 49.

<sup>26</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, Uzun v Germany, case no. 35623/05, § 52.

<sup>27</sup> The application of geolocation surveillance was based on Article 100c § 1 point 1 (b) of the German Code of Criminal Proceedings. EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010*, Uzun v Germany, case no. 35623/05, § 64 and 65.

<sup>28</sup> *Ibidem*, § 71.

of conversations - it is not necessary for the judicial authority to decide on the collection of location data<sup>29</sup>. Due to the allegations made against the applicant - participation in a terrorist group, attempted murder - the use of covert surveillance measures was justified on the grounds of protection of public safety, in particular by preventing new (terrorist) bomb attacks. Moreover, the previously-used less invasive investigative techniques did not bring the expected results (they did not prevent the applicant from committing new crimes)<sup>30</sup>. Considering the circumstances of the case, the actions of law enforcement agencies, the procedural guarantees that German legislation provided for people who were subject to covert surveillance and the fact that the investigative steps taken were necessary in a democratic society, the ECtHR found that there had been no violation of Art. 8 sec. 1 of the ECHR.

The Strasbourg Court also dealt with the issue of collecting data on the location in the judgement of *Ben Faiza against France*<sup>31</sup>. In this judgment, the ECtHR relied on the *Uzun v Germany* judgement, using the principles developed there. Compared to the previous decision, the novelty was to draw attention to the fact that geolocation monitoring may be applied in two forms: by means of a GPS device installed, for example, directly in a car or other means of transport, or by using its own telephone technology (smartphone), tablet or GPS system included with the car<sup>32</sup>. When analysing French law, the ECtHR noted that, at the time when geolocation surveillance was applied to the applicant, the provisions were not precise enough. The provision of art. 81 of the French CCP

---

<sup>29</sup> *Ibidem*, § 73.

<sup>30</sup> *Ibidem*, § 79-80.

<sup>31</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, *Ben Faiza v France*, case no. 31446/12. The case concerned the allegation of involvement in an organised criminal group and drug trafficking and smuggling. Apart from geolocation surveillance, other means of covert surveillance were used against the complainant, such as interception, transmission and recording of calls. See: § 54.

<sup>32</sup> At the time when geolocation surveillance was applied in the *Uzun v. Germany* case, the technology was not yet at such a high level, including smartphones that automatically collect location data. EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, *Ben Faiza v France*, case no. 31446/12, § 53.

referred to “informational activities useful for revealing the truth”<sup>33</sup>. This regulation did not ensure the predictability of the proceedings within the meaning of Art. 8 of the ECHR - it did not define the conditions and rules for collecting location data with sufficient precision - and the jurisprudence of French courts did not develop mechanisms that would protect individuals against unjustified interference with the right to privacy. Due to the defectiveness of the legislation in force in France at the time, the Court found that there had been a violation of Art. 8 of the ECHR, without considering whether the application of geolocation surveillance was necessary in a democratic society and served the purposes of Art. 8 sec. 2 of the ECHR<sup>34</sup>.

### 3.2. REAL-TIME DATA COLLECTION IN THE EU LAW AND CJEU JURISPRUDENCE

Legislation adopted in the EU requires EU member states to adopt “effective investigative tools” in relation to organised crime and other serious crime, including money laundering<sup>35</sup>, sexual crimes against children<sup>36</sup> (sexual abuse, sexual exploitation, child pornography,

<sup>33</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, Ben Faiza v France, case no. 31446/12, § 58.

<sup>34</sup> Following the conclusion of the applicant’s case, regulations were introduced in France in 2014 which clarified the application of geolocation surveillance and provided procedural guarantees for the individual to prevent unauthorised interference with the right to privacy. EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018*, Ben Faiza v France, case no. 31446/12; § 39.

<sup>35</sup> DIRECTIVE (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, published in the Official Journal of the European Union no. L 141/73 of 5 June 2015. eur-lex.europa.eu. Access on December 20, 2020.

<sup>36</sup> DIRECTIVE (EU) 2011/92 of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA published in the Official Journal of the European Union no. L 335/1 of 17 December 2011, eur-lex.europa.eu. Access on December 20, 2020.

solicitation of children for sexual purposes), illegal drug trafficking<sup>37</sup>, trafficking in human beings<sup>38</sup> or protection of the EU's financial interests. One such "effective tool" is real-time location data tracking. For the first time, the issue of real-time geolocation supervision was dealt with by the Luxembourg Court in the case of *La Quadrature du Net and the Others*<sup>39</sup>, and in its ruling it took into account the position of the ECtHR, recognising the Strasbourg standard as the minimum EU standard<sup>40</sup>.

Contrary to the cases heard by the Strasbourg court, the CJEU examined French regulations that obliged electronic service providers to retain and process - in an automated manner - data on the location of persons who were suspected of committing a serious crime or posing a threat to national security<sup>41</sup>. However, the Luxembourg Court noted that in practice, this led to real-time geolocation surveillance being extended to all electronic communications users - irrespective of whether the person was actually involved in any prohibited act. Although location

---

<sup>37</sup> COUNCIL FRAMEWORK DECISION 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking; published in the Official Journal of the European Union no. L 335/8 of 25 October 2004, eur-lex.europa.eu. Access on December 20, 2020.

<sup>38</sup> DIRECTIVE (EU) 2011/36 of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, published in the Official Journal of the European Union no. L 101/1 of April 2011, eur-lex.europa.eu. Access on December 20, 2020.

<sup>39</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net* (hereinafter: *La Quadrature du Net and the others*). <http://curia.europa.eu/>.

<sup>40</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net*, § 124.

<sup>41</sup> See: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net*, § 41-45. Those regulations was introduced to prevent and fight with terrorist crime.

data was collected anonymously, it was possible to identify the user if this information was relevant to the criminal proceedings<sup>42</sup>.

The CJEU found that the automated geolocation surveillance of the almost unlimited number of users of electronic communications goes beyond what is necessary to ensure national security. It is necessary to apply criteria limiting the number of people subject to discrete geolocation surveillance<sup>43</sup>. The earlier agreed models of automatic data processing and the criteria of those people against whom geolocation surveillance may be used, should be specific and credible (enabling the achievement of results identifying persons with a justified suspicion of involvement in terrorist offences) and non-discriminatory. There is a need for prior judicial review or other independent body to assess whether automatic retention of location data is acceptable in a given case<sup>44</sup>. If the information obtained as a result of automatic mass data retention provided information essential for maintaining national security (e.g. that thanks to it, members of an organised terrorist group were identified), the possibility of their use in a criminal trial depends on the subsequent assessment of the court. An individualised, non-automated analysis is required as to whether discreet geolocation surveillance and data collection have been carried out in accordance with the law and served the purposes provided for by this law<sup>45</sup>.

---

<sup>42</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, § 185-187. The CJEU referred to the ECtHR judgment in case *Ben Faiza v France*.

<sup>43</sup> However, this time may be extended if necessary in a specific case.

<sup>44</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, § 183-189.

<sup>45</sup> *Ibidem*. It is also worth mentioning that the CJEU requires regular publication of general information (reports) on the scale of secret geolocation surveillance. Individual notification of persons who have been subject to such supervision is not necessary. However, if the automatic analysis of location data is 'deepened', i.e. a specific individual is identified and his behaviour is further analysed, he should be informed that he has been subject to secret surveillance. However, such information must not affect the tasks of process authorities. See: *ibidem*, § 190-192.

### 3.3. PARTIAL CONCLUSIONS

Summing up, when it comes to collecting real-time location data, it is difficult to speak of a developed European standard at this stage. The Strasbourg case-law cannot be considered as developed - the ECtHR has dealt with this issue only twice. Nevertheless, at a very general level, it is possible to determine what conditions should be met by national law so that the interference with the privacy of an individual as a result of geolocation supervision does not lead to violation of Art. 8 sec. 1 of the ECHR. Firstly, the collection of location data is not “reserved” exclusively for serious crime and may also be used in more common criminal offences. The ECtHR considers geolocation supervision to be a measure less intrusive to the privacy of an individual than other forms of covert surveillance, which allow, *inter alia*, to record the content of conversations or the image of a given person. Consequently, this form of collecting data about an individual may be used in a greater number of cases. Secondly, the Court emphasises the need to introduce procedural guarantees that will prevent abuse and unjustified interference with the privacy of an individual. National legislation should specify:

1. material scope, i.e. in cases of what crimes geolocation surveillance can be applied,
2. the subjective scope, i.e. the categories of people for whom real-time geolocation surveillance can be used, should be defined,
3. temporal scope, i.e. the maximum period during which real-time tracking of the individual’s movement is allowed.

Thirdly, geolocation surveillance does not have to be ordered by a judicial authority and the ECtHR considers that judicial control at the stage of assessing the admissibility of using location data is sufficient. The court should check not only whether the statutory conditions for geolocation surveillance have been formally met, but also assess whether such action was “necessary in a democratic society”.

The Court of Justice of the European Union has so far dealt with the problem of mass, automated retention and processing of location data of an unlimited group of users in order to ensure national security.

It has allowed for the possibility of automated analysis and collection of location data and the obligation for electronic service providers to transmit this data to procedural authorities, but such activities must be limited to situations where there is a serious threat to national security and it is necessary to ensure effective judicial or independent administrative control. In addition, the collection of real-time traffic and location data must be restricted to only persons reasonably suspected of being involved in terrorist activities, to the extent strictly necessary to ensure national security. National legislation should provide for a maximum period of application of covert geolocation surveillance, but it may be extended - in particularly justified situations.

#### **4. COLLECTING LOCATION DATA FROM PROVIDERS OF ELECTRONIC COMMUNICATIONS SERVICES**

##### **4.1. COLLECTING LOCATION DATA FROM PROVIDERS OF ELECTRONIC COMMUNICATIONS SERVICES – THE ECtHR JURISPRUDENCE**

The Strasbourg Court first dealt with the issue of access to location data stored by mobile network operators in the judgement of Ben Faiza against France<sup>46</sup>, which emphasised that any data collection and retention related to the use of a telephone without the knowledge of the person concerned, constitutes an interference with the right to respect for private life under the article 8 of the ECHR<sup>47</sup>. It is necessary to distinguish between situations in which state authorities create a system of surveillance of an individual and monitor their behaviour “on an ongoing basis” from the transfer of information obtained by that entity by a private entity, if it is necessary to establish the circumstances of a criminal case. In the opinion of the ECtHR, obtaining *a posteriori* access

---

<sup>46</sup> It is worth to mention that the ECtHR referred to previous judgments in cases of the access to list of telephone calls. See: EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 1 March 2007, Heglas v the Czech Republic*, case no. 5935/02, § 61; EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 December 2009, Previti v Italy*, case no. 45291/06, § 303.

<sup>47</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018, Ben Faiza v France*, case no. 31446/12.

to location data constitutes less interference with the right to privacy than monitoring the individual's movement in real time<sup>48</sup>. Nevertheless, the duty of state authorities is to comply with the general rules allowing for interference in the private sphere, i.e. such interference must be grounded in national law and serve the purposes of art. 8 sec. 2 of the ECHR and fulfil the condition of necessity in a democratic society. When assessing the French legislation, the Court found that there had been no violation of Art. 8 sec. 1 of the ECHR. The regulations specified which authority could turn to the mobile network operator, in which cases this measure was admissible, and the use of location data was subject to judicial review<sup>49</sup>. There was also an important public interest justifying the interference with the individual's right to privacy. The applicant was charged with serious crimes - participation in an organised criminal group and drug trafficking, and the information obtained thanks to geolocation data was necessary to establish the truth in the trial.

In the decisions of *Ringler vs. Austria*<sup>50</sup> and *Tretter and others vs. Austria*<sup>51</sup>, the ECtHR assessed the Austrian provisions allowing procedural authorities to request mobile network operators to disclose personal data, e.g. location data, list of calls, personal data of the user of a given telephone number, and IP address<sup>52</sup>. In order to obtain data from the network operator, the law enforcement authorities had to adequately justify such a request, indicating that there is a threat and that the data is necessary for the performance of police tasks. With regard to location data, it was necessary to indicate that there was a direct threat to the life

---

<sup>48</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018, Ben Faiza v France*, case no. 31446/12, § 71.

<sup>49</sup> *Ibidem*, § 79. The court assessed whether recourse to the mobile network operator was lawful and, if it considered it was not, it had the right to exclude the material thus obtained from the evidence base.

<sup>50</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10.

<sup>51</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10.

<sup>52</sup> See: the Article 53 sec. 3a and 3b Sicherheitspolizeigesetz. See also: EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, § 4-23.



or health of a specific person. Subsequent changes to the regulations<sup>53</sup> extended the possibility of requesting access to location data to include situations where there is a direct threat to the freedom of a person. In such a situation, the procedural authorities could ask for geolocation information of the person who was in danger (the aggrieved party), and not only the person suspected of committing a crime<sup>54</sup>. Austrian regulations guaranteed the person whose data had been transferred to law enforcement authorities the right to submit a request for information on the actions taken against him and the sharing of data with the police authorities, he could request the deletion of data, and the supervision of the correct disclosure and processing of personal data was exercised by an independent authority<sup>55</sup>. In the *Ringler and Tretter and Others vs. Austria* cases, the applicants argued that the provisions did not provide for an effective measures in protecting individual rights and freedoms<sup>56</sup>. The mechanism of notifying the transfer of personal data (including location data) was questioned. According to the complainants, it cannot be expected that the individuals will regularly request state authorities to provide information on whether their personal data has been transferred to the police authorities in connection with ongoing

---

<sup>53</sup> Amendments were introduced on 1 April 2012, 1 April 2014, 1 June 2016 and 25 May 2018 due to obligation to implement the EU directives, especially the directive 2016/680, and REGULATION (EU) 2016/679 of European Parliament and 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; published in the Official Journal of the European Union no. L 119/1 of 4 May 2016) which has entered into force on 25 May 2018.

<sup>54</sup> The amendments have extended the possibility of requesting the data of a mobile phone user, also in order to avoid endangering life, health or freedom, to avoid an intentional crime or to stop the activities of criminal groups. EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, § 23. See also: EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10, § 18.

<sup>55</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10, § 34.

<sup>56</sup> In the meaning of the Article 13 ECtHR.

criminal proceedings<sup>57</sup>. Moreover, the regulations allow one to request access to geolocation data in any circumstances - the regulations do not impose any restrictions<sup>58</sup>. The victim's status<sup>59</sup> was justified by the inability to prove that the applicants had been subject to covert surveillance measures and their personal data (including location data) had been transferred to the police<sup>60</sup>.

In *Ringler vs. Austria* and *Tretter and the other vs. Austria* cases the ECtHR recalled that its role was not to summarise the national law of a country or the practice of procedural authorities, but to establish whether, in a particular case, the application of national regulations had led to a violation of the Convention<sup>61</sup>. Nevertheless, the specific characteristics of covert surveillance measures mean that an individual may sometimes rely on the fact that he or she is a victim of the very existence of covert surveillance provisions, even if he is unable to demonstrate that such measures were applied to him<sup>62</sup>. In assessing whether this is the case, the Court takes into account:

1. the scope of application of the provisions allowing for a covert interference in an individual's privacy (objective, subjective and temporal), whether such measures could potentially be applied to the complainant due to belonging to a specific category of persons to whom national provisions apply, or examines whether the provisions have a direct impact on all users of electronic communications:

---

<sup>57</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10, § 58.

<sup>58</sup> *Ibidem*, § 52.

<sup>59</sup> In both cases the Austrian Government contested the victim status of the applicants.

<sup>60</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10, § 47-50. EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, § 55.

<sup>61</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, § 58 and further the ECtHR jurisprudence.

<sup>62</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 12 January 2016, Szabó and Vissy v Hungary*, case no. 37138/14, § 33.

2. availability of domestic remedies; Where there is no possibility at national level to challenge the use of covert surveillance measures, public fears that power may be abused may be justified, and therefore the ECtHR needs to be scrutinised<sup>63</sup>.

The ECtHR agreed with the applicants that the right to request information as to whether an individual had been subjected to covert surveillance measures was of no practical importance<sup>64</sup>. However, it noted that law enforcement authorities were required to notify an independent authority about requests made to mobile network operators. The authority is obliged to inform the person - upon his / her request - about any unlawful measures that were applied against him, and if he refuses to provide information - the person may submit a complaint to an independent commission whose decisions are subject to judicial review<sup>65</sup>. It may also demand the deletion, rectification or limitation of the processing of personal data, if they are no longer needed to protect public security. Apart from the supervisory authority of the protection of personal data, the personal data protection commission and the judicial control of decisions issued by the commission, the system of measures to protect individual rights is supplemented by the institution of the Legal Protection Commissioner, who has the right to access and control the correct application of the provisions on the protection of personal data<sup>66</sup>.

In the cases of *Ringler and Tretter and others vs. Austria*, the Court dismissed the complaints, questioning the applicants' victim status. Nor did he find that there were grounds for an abstract review of Austrian legislation. It is worth noting, however, that although the ECtHR stated that it did not assess *in abstracto* the legislation of the countries of the Council of Europe, in fact - as if in response to the complainants' allegation - it assessed that the Austrian provisions guarantee effective means of protecting an individual against unauthorised interference with

---

<sup>63</sup> *Ibidem*, § 36.

<sup>64</sup> The ECtHR has taken into account the scope of exceptions that allow non-disclosure of such information.

<sup>65</sup> EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, § 44.

<sup>66</sup> *Ibidem*, § 78.

the right to privacy. Although he found some mechanisms (e.g. informing an individual about the use of covert surveillance measures against him / her to be burdensome and even devoid of practical significance), due to the existence of an independent system of supervision over the correct processing of personal data, the ECtHR found that the measures available at the national level to protect individual rights and freedoms are sufficient, and therefore no Strasbourg intervention is necessary. However, it should be emphasised that when assessing the Austrian regulations, the Court essentially examined the compliance of EU solutions regarding the protection of personal data, including location data, introduced by Directive 2016/680.

At present, it appears that the Strasbourg Court is avoiding taking a position on the issue of access to location data collected by mobile operators. The rules that the ECtHR has developed in relation to access to the lists of calls made by the telephone user cannot be applied analogously. This is because location data provides other types of information to procedural authorities and are used for a different purpose. Billing data provides information on who the person contacted, how long the call lasted, and how many times it was made within a certain period of time. Location data refer to the places where a given person has been, they allow to determine their pattern of behaviour. They interfere with the privacy of an individual to a greater degree than the list of calls. It is difficult to determine, solely on the basis of the judgement of *Ben Faiz vs. France*, what are the requirements of the ECtHR with regard to the countries of the Council of Europe regarding the regulation of the issue of access to location data. In the decisions of *Ringler and Tretter and others vs. Austria*, the Court did not present its own position, but only held that Austrian solutions - implementing EU solutions - were compatible with the Convention.

#### **4.2. COLLECTING LOCATION DATA FROM PROVIDERS OF ELECTRONIC COMMUNICATIONS SERVICES – THE EU LAW AND THE CJEU JURISPRUDENCE**

Much attention is paid to the issue of collecting and sharing location data with procedural authorities in relation to the prevention

and combating crime in EU law and the jurisprudence of the CJEU<sup>67</sup>. The provision of the Article 5 of Directive 2002/58 introduces the principle of confidentiality of communications, including the confidentiality of location data. Derogations from this principle are possible for the purposes of ensuring national security, state security, defence, public safety and for the purpose of detecting, investigating and punishing criminal offences (Article 15 of Directive 2002/58). National law must ensure that the investigative measures used in a specific case are necessary, appropriate and proportionate in a democratic society. The clause limiting the confidentiality of location data is exhaustive and cannot be interpreted extensively. Location data is retained in accordance with EU law, provided that the purpose of this activity is to fight crime<sup>68</sup>. These data may be transferred (made available) to state authorities on the terms - and with the guarantee of individual rights - specified in Directive 2016/680. Sharing data is allowed only for the purposes of preventing or combating crime, at the request of a given person, he should be provided with information whether his personal data (including location data) have been processed by the police<sup>69</sup>, and he

---

<sup>67</sup> See: Zob. szerzej: DOCKSEY, Christopher. Ministerio Fiscal: Holding the line on ePrivacy. *Maastricht Journal of European and Comparative Law*, vol. 26, no. 4, p. 585–594, 2019; THIERSE, Stephen. The Never-Ending Story of Data Retention in the EU, [in:] THEIERSE, Stephen, BADANJAK, Sanja. *Opposition in the EU Multi-Level Polity. Legal Mobilization against the Data Retention Directive*. Springer 2020, p. 11-26; ZUBIK, Marek, PODKOWIK, Jan, RYBSKI, Robert. Prywatność. Wolność u progu D-day. *Gdańskie Studia Prawnicze*, t. XL, p. 391-408, 2018, OJANEN, Tuomas. Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, *European Constitutional Law Review*, v. 10, no. 3, p. 528-541; MURPHY, Maria Helen. Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger. *Irish Criminal Law Journal* t. 105, v. 24, no. 4, 2014; CELESTE, Edoardo. The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios. *European Constitutional Law Review*, no. 15, p. 134–157, 2019.

<sup>68</sup> OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona, delivered on 15 January 2020, case no. C-520/18; <http://curia.europa.eu/>.

<sup>69</sup> See: article 13 and 14 of the directive 2016/680. The limitation of those rights: see: the Article 15 of the directive 2016/680. A person shall be informed ex officio if the violation of personal data involves a threat to his or her life, health or safety. See: the Article 31 of the Directive 2016/680.

may request the deletion of his data if it is useless to achieve the objectives referred to in the directive, or they are obsolete or have been obtained unlawfully<sup>70</sup>. Control over the correctness of personal data processing in connection with the prevention and combating of crime should be exercised by an independent authority, and the individual concerned - if his/her data has not been deleted despite the request or considers that it is being processed unlawfully - may bring the matter to court<sup>71</sup>.

However, EU regulations do not specify in which cases location data can be obtained, nor do they indicate how long this data can be stored. The provision of the Article 15 of the Directive 2002/58 indicates that the data collected by service providers may be transferred to law enforcement authorities in order to combat “criminal offences”, and the Article 5 of the Directive 2016/680 requires EU countries to introduce “appropriate deadlines for the deletion of personal data or for periodic review of the necessity to retain personal data”. The EU legislator has left the Member States a margin of discretion in regulating the issue, i.e. in what cases and for what purposes the data will be collected, and for what period of time they will be stored. However, Member States’ freedom of implementation is controlled by the EU Court of Justice.

In the *Tele2 and Watson* judgement<sup>72</sup>, the CJEU assessed the rules in force in Sweden and the United Kingdom. The law in force in Sweden obliged the provider of electronic communications services to provide - at the request of the prosecutor’s office, the police or another authority responsible for combating crime - the subscriber’s data if they relate to an alleged infringement, without the subject of criminal proceedings having to be a “serious crime”<sup>73</sup>. The solutions

---

<sup>70</sup> See: the Article 16 of the Directive 2016/680.

<sup>71</sup> See: the Article 17 sec. 3 of the Directive 2016/680.

<sup>72</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 21 December 2016*, C-203/15 and C-698/15. The courts referred questions for a preliminary ruling after the CJEU judgment in *Digital Rights Ireland* annulled the so-called Retention Directive, and the regulations in force in Sweden and the United Kingdom in connection with which the question was referred for a preliminary ruling were the implementation of the above directive.

<sup>73</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 21 December 2016*, C-203/15 and C-698/15, *Tele2 and Watson*, § 25. The question of the Sweden Court: see § 51.

adopted in the United Kingdom did not specify the scope of access to location data<sup>74</sup>. The body established to prevent and combat crimes had the right to request the mobile network operator to disclose data due to: national security, economic interests of the state, protection of public health, the need to prevent or detect crimes or to prevent violations of public order, to determine the size or collection of taxes, levies, fees or other obligations, contributions or charges due to a state administration unit, emergencies, in order to prevent injuries or damage to the physical or mental health of a person, or to reduce the extent of damage to a person's physical or mental health. In addition, the minister of the interior could, by order, specify other situations in which state authorities could gain access to location data.

In the judgement of *Tele2 and Watson*, the EU Court of Justice recalled that under the Article 5 of the Directive 2002/58, the protection of the confidentiality of electronic communications is intended to prevent any unlawful access to data, including data related to a message (i.e. location data)<sup>75</sup>, irrespective of whether such access could be obtained by public (state) or private entities. The provisions imposing an obligation on telecommunications service providers to provide data fall within the scope of Art. 5 of Directive 2002/58. The CJEU has formulated general rules for data retention, including location data, and then for their transfer to trial authorities. Firstly, clear and precise rules should be introduced in national law regarding the scope and manner of the data storage measure to be applied. The way in which the concept of “national security” is understood in the EU countries does not fall within the scope of the CJEU. However, the Luxembourg Court assesses whether the law in force in a given state does not allow for unauthorised and disproportionate interference with the right to privacy of an individual<sup>76</sup>. Secondly, data retention must be carried out on the basis of objective criteria that show the link between the data that has been retained and the legitimate purpose for which the retention

---

<sup>74</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 21 December 2016*, C-203/15 and C-698/15, § 33. The question of the Sweden Court: see § 59.

<sup>75</sup> *Ibidem*, § 77.

<sup>76</sup> *Ibidem*, § 94-96.

is intended. Third, these criteria must enable the identification and tracking of persons who have, even indirectly, a connection with serious crime. National regulations that ensure universal access to the retained data are inconsistent with EU law, regardless of the existence of any connection with one of the purposes indicated in art. 15 of Directive 2002/58. The generalised and non-differentiated obligation to retain all traffic and location data of all subscribers and users disproportionately violates the fundamental rights of Articles 7, 8 and 11 of the Charter<sup>77</sup>. Users of telecommunications networks cannot be under the constant state surveillance and they should not be afraid that their every move is tracked, registered and may be used against them in the future. In addition, it is necessary to introduce a storage date for location data - it is unacceptable to store information about an entity longer than necessary to ensure public safety.

In response to the preliminary questions, the CJEU questioned the solutions in force in Sweden and the United Kingdom and ruled that the Article 15 par. 1 of the Directive 2002/58 in conjunction with the Articles 7, 8, 11 and art. 52 sec. 1 of the Charter of Fundamental Rights of the European Union should be interpreted in such a way that it precludes national legislation:

- providing for generalised and non-differentiated retention of all traffic data and location data of all subscribers and registered users of all electronic means of communication for the purposes of combating crime; and
- concerning the protection and security of traffic and location data, and in particular access by competent national authorities to stored data, which, in the context of combating crime, does not restrict such access only for the purpose of combating serious crime, and does not make the granting of such access conditional from prior control by a court or an independent administrative authority and do not require that the data be stored within the Union.

---

<sup>77</sup> See also: OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona, delivered on 15 January 2020, case no. C-520/18, § 72.



The issue of obtaining access to location data was also resolved in the Privacy International case<sup>78</sup>. The basis for a request by the British court for a preliminary ruling<sup>79</sup> was the doubt whether the provisions allowing the mass acquisition of telecommunications data regarding traffic and location of the individual from providers of electronic communications services<sup>80</sup> on the basis of orders issued by the secretary of state to use such collected information to ensure state security<sup>81</sup> are consistent with EU law<sup>82</sup>. British regulations allowed for undifferentiated and generalised access to location data. In order for geolocation information to be passed on to the security services, it was not necessary to prove that the person was related to an activity that could pose a threat to national security.

The CJEU reminded that any interference with the privacy of an individual must meet the condition of proportionality<sup>83</sup>. Limitation of privacy may occur within strictly defined limits and only when it is necessary to achieve a legitimate aim (e.g. ensuring public security,

---

<sup>78</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17.

<sup>79</sup> The preliminary question; see: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, § 29.

<sup>80</sup> The data was gathered by the British Secret Services: MI5, MI6, GCHQ. See: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, § 20

<sup>81</sup> See also: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17; § 16-18. The British, Hungarian, Polish, Czech Republic governments have raised objections, pointing out that national security is an exclusive matter for Member States and does not fall within the scope of Directive 2002/58, so the EU CJ has no jurisdiction to rule on it. See also: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18, § 87-103.

<sup>82</sup> The Directive 2002/58.

<sup>83</sup> The problem of the proportionality of interference with the right to privacy - with regard to telephone user/consumer data - was examined by the CJEU in the case *Minister Fiscal*. See: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 2 October 2018, Ministerio Fiscal*, C-207/16, § 55. An interference with the rights of the individual may be considered proportionate if, given the seriousness of the offence, the circumstances of the case, it is more beneficial - from the perspective of the general public - to restrict the rights of the individual.

fighting crime)<sup>84</sup>. These goals cannot be pursued at all costs, i.e. without taking into account and respecting the rights of an individual<sup>85</sup>. Legal regulations allowing for the intrusion into the privacy of an individual must meet the conditions of specificity, i.e. indicate the grounds and scope of the restriction (i.e. what data will be processed) and provide for procedural guarantees that will reduce the risk of abuse. It is about creating effective mechanisms that will ensure that data will be processed only to the extent that it is necessary<sup>86</sup>. It is worth emphasising, however, that the EU Court of Justice indicated that the goal of ensuring national (public) security allows for further restrictions on fundamental rights than combating crime, including serious crimes. State authorities must have adequate and effective methods of obtaining information about possible threats that could destabilise the state's activity - constitutional, political or social structures in the country - and directly threaten society and the population<sup>87</sup>. However, the pursuit of national security does not allow for general, universal and undifferentiated collection and processing of location data. In response to a question from a British court, the Luxembourg Court found that the provisions in force in the United Kingdom were incompatible with EU law. It indicated that the Article 15 sec. 1 of the Directive 2002/58 in connection with the Article 4 sec.

---

<sup>84</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17; § 77.

<sup>85</sup> The private interest and the interest of the general public must be properly balanced. A priori it cannot be assumed that ensuring public safety and public security in every case is more important than the rights and freedoms of an individual. See: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, § 67 and COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 8 April 2020, Digital Rights Ireland*, C-293/12 and C-594/12, § 52.

<sup>86</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, § 74; COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18, § 132.

<sup>87</sup> These include terrorist activities. See: COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, § 74; COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18, § 135.

2 TEU<sup>88</sup>, as well as the Article 7, 8 and 11 and 52 sec. 1 of the Charter of Fundamental Rights of the European Union, “must be interpreted as precluding national legislation enabling a state authority to impose on providers of electronic communications services a generalised and non-differentiated obligation to transmit traffic and location data to intelligence and security services for national security protection purposes”.

The problem of bulk retention of location data was also analysed in the judgment of *La Quadraturedu Net and the Others*<sup>89</sup>. In these proceedings, the Luxembourg Court examined French and Belgian legislation which allowed for the preventive retention of traffic and location data in order to ensure public safety and prevent serious crimes<sup>90</sup>. Nevertheless, even if location data is preventively retained to ensure national security, such actions by state authorities must be limited to what is absolutely necessary. It is necessary to introduce restrictions (e.g. by establishing the subjective and temporal scope) and safeguards that will enable effective protection of the data of persons for whom the data has been disclosed to state authorities against the risk of abuse<sup>91</sup>. Systematic, continuous and unlimited retention of location data is unacceptable. In addition, decisions obliging providers of electronic communications services to retain location and traffic data and then transfer them to state authorities should be subject to effective review by a court or an independent administrative authority, which will be able to assess the legality of actions taken by procedural authorities<sup>92</sup>. With regard to the

---

<sup>88</sup> The Treaty on European Union; consolidate version published in the Official Journal no C 326 on 26 October 2012. Access on December 20,2020. <https://eur-lex.europa.eu/>.

<sup>89</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18.

<sup>90</sup> One of the positive obligations of the state from the Article 8 of the ECHR and Article 7 of the Charter is the introduction of appropriate substantive and procedural provisions which will make it possible to effectively combat serious crime and ensure universal security.

<sup>91</sup> COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18, § 138.

<sup>92</sup> *Ibidem*, § 139.

implementation of the goal of ensuring universal security, the CJEU allowed - under the above-mentioned conditions - preventive retention and collection of location data. Conversely, the massive, preventive retention of location and traffic data for the purposes of crime prevention, investigation, detection and prosecution is unacceptable. The Court found that national legislation which provides for the general and non-differentiated retention of these data goes beyond what is necessary to combat serious crime and cannot be justified in a democratic society<sup>93</sup>. French and Belgian legislation allowed for the retention of location data of all users of electronic communications services, even if they were not, even indirectly, in a situation that could lead to criminal proceedings against them. These regulations also included persons whose behaviour did not pose any threat to public safety<sup>94</sup>. It does not matter whether the retained data was used in subsequent criminal proceedings. It is important that the procedural bodies entered the sphere of privacy of the individual, violating the confidentiality of communication, expressed in the Article 5 of the Directive 2002/58<sup>95</sup>. The very possibility of accessing personal data is an interference with the right to privacy.

The CJEU formulated general conditions as should be met by the national laws of European Union member states. It is necessary to introduce time, geographic and subjective restrictions - data may be retained on the location of persons suspected of committing a serious crime, persons otherwise involved in criminal activity and persons who could, for other reasons, contribute to the fight against serious crime<sup>96</sup>. Geographical and subject restrictions must be established on the basis of objective and non-discriminatory factors<sup>97</sup>. The retention

---

<sup>93</sup> *Ibidem*, § 141.

<sup>94</sup> *Ibidem*, § 143.

<sup>95</sup> *Ibidem*, § 116.

<sup>96</sup> E.g. husband, wife or other close relatives to members of criminal groups (organized crimes groups).

<sup>97</sup> On the geographical scope, the Court pointed out that these are areas with a high risk of serious crime, such as urban infrastructure regularly visited by large numbers of people, or strategic locations such as airports or railway stations. COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, La Quadrature du Net and the Others*, C-511/18, C-512/18 and C-520/18, § 150.

time of the location data must not exceed what is strictly necessary for the intended purpose.

### 4.3. PARTIAL CONCLUSIONS

In conclusion, the Luxembourg and Strasbourg courts consider that access to ex post location data - previously retained by mobile network operators - is an interference with the right to privacy (the Article 8 of the ECHR, the Article 7 of the Charter). However, this interference is permissible if there are appropriate legal bases in national law, its purpose is to protect the values expressed in the Article 8 sec. 2 of the ECHR and, moreover, has been limited to what is necessary in a democratic society. The ECtHR and the CJEU considered the problem of retention and access to geolocation data from different perspectives. The Strasbourg Court assessed whether, in a specific case, the application of domestic provisions did not result in a violation of the Article 8 of the ECHR. In the *Ringler and Tretter and others vs. Austria* cases, the applicants tried to induce the ECtHR to analyse abstractly the domestic provisions allowing - in practice - the massive collection of location data. In this regard, the Court did not reply to the applicants. While examining the system of national measures to protect the rights and freedoms of individuals - introduced in connection with the need to implement EU regulations - it concluded that they allow for the enforcement of effective protection of the right to privacy in 'state' proceedings, so Strasbourg intervention is not necessary.

The Luxembourg Court assessed the regulations of the European Union countries that allowed for the mass retention of data on the location of users of telecommunications networks<sup>98</sup>. It was possible to obtain geolocation information about any person, regardless of whether they were involved, even indirectly, with any crime. The introduction of such regulations was justified by the need to protect and ensure national security as well as the prevention and combating of serious crime.

---

<sup>98</sup> The Court considered that the blanket and indiscriminate obligation to retain all traffic and location data of mobile phone users disproportionately interferes with the fundamental rights protected under Articles 7, 8 and 11 of the Charter.

However, the CJEU recognised that any personal data retention system (including location data) must be organized in such a way that it cannot be transformed into an undifferentiated and general collection of information about individuals<sup>99</sup>. Society cannot be under constant surveillance of state organs. The fight against terrorism and the protection of national security cannot be considered only taking into account the criterion of the effectiveness of actions taken. Each time, the insurmountable limit is respect for the rights of individuals and finding the right balance between the common good and the sphere of individual rights and freedoms. Retaining location data is possible, but on the condition that:

1. clear and precise rules have been introduced regarding the scope and method of data retention, processing and storage (subject, geographic and temporal limitations);
2. there are objective criteria defining the link between the data to be retained and stored and the legitimate purpose (combating serious crime, protecting national security);
3. they concern people who are involved - even indirectly - with serious crime, and at the same time there are mechanisms protecting against obtaining data about the location of other people not involved in criminal activity<sup>100</sup>.

## 5. CONCLUSIONS

Obtaining information about the location by state authorities and the related analysis of the routine of an individual's life is an interference with the right to privacy (the Article 8 of the ECHR, the Article 7 of the Charter). Due to the development of technology, law enforcement authorities of a given state can easily collect data relevant to the conducted proceedings. Almost every person uses a mobile phone (smartphone) with

---

<sup>99</sup> OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona delivered on 15 January 2020, C-623/17, Privacy International. <http://curia.europa.eu/>.

<sup>100</sup> OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona delivered on 15 January 2020, C-623/17, Privacy International. <http://curia.europa.eu/>. See also: OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona delivered on 15 January 2020, C-520/18.

GPS, so the services responsible for public safety no longer need to install separate transmitters to track (reproduce) the behaviour of a given person. The ease of obtaining information about the location and its usefulness for achieving the goal of combating and preventing crime, ensuring public safety, gives rise to the risk of abuse. Although the right to privacy is not an absolute right and is subject to limitations due to the overwhelming social (public) interest, it is necessary to properly balance the interests of the individual and society. European courts try to define the relationship between respecting fundamental rights and the obligation to prevent and combat serious crime. Based on the jurisprudence of the ECtHR and the CJEU, it can be deduced in which circumstances the collection of location data does not violate the fundamental rights of an individual.

Compared to other investigative techniques, the collection of location data violates the right to privacy to a lesser extent than, for example, control and recording of conversations or audiovisual observation. The Luxembourg and Strasbourg Courts recognise the acquisition of geolocation data in real time as a more painful method (interfering in a greater scope in the right to privacy of the individual) from obtaining ex post location data from mobile network operators. The degree of interference with the right to privacy and the affliction of a given method affect the material scope (in which cases such methods are permissible), the subjective scope (determining the group of people whose location data can be obtained), and temporal (how long a given measure can be used).

Regarding the collection of real-time location data, the ECtHR stresses that the use of this covert surveillance method is only permissible in connection with serious crime. The decision to apply geolocation surveillance to a specific person does not have to be taken by a judicial authority. Ex-post judicial control is sufficient, i.e. at the stage of assessing whether the geolocation data has been obtained lawfully and whether it can be used as evidence in criminal proceedings. The Strasbourg Court draws attention to the existence of clear and precise provisions in domestic law, specifying the basic principles and conditions for the application of geolocation surveillance, and assesses whether in a specific case the collection of location data served one of the purposes set out in the Article 8 sec. 2 of the ECHR.

Striving to protect national security, combating serious crime, etc. does not entitle state authorities to massive and automated real-time monitoring of an entire society. A person or group of persons to whom geolocation surveillance is applied must be associated - even indirectly - with criminal activity that poses a threat to public security. The European Union Court of Justice in the judgement of *La Quadrature du Net and the Others* emphasised that collecting location data for groups is admissible, provided that such action serves solely the protection of national security. It is necessary to introduce regulations that will minimise the risk of abuse. The decision to include a group of people under automated geolocation must be taken by a judicial authority or other independent body, and then, before the location information is used as evidence in the proceedings, a personalised ex-post control by the court is necessary. However, it should be emphasised that the Luxembourg Court ruled out the possibility of using automated, continuous monitoring of the movement of groups of people in order to combat crime, but on the condition that data collected by automated means are subject to non-automated analysis before being used in the future.

Obtaining location data ex post, i.e. from mobile network operators constitutes less interference with the right to privacy. Procedural authorities may, in individual cases, request geolocation information not only when the subject of the proceedings is a serious crime, but also in relation to prohibited acts of a lower gravity. However, national law may not require mobile network operators to retain location data in a compulsory manner. It is necessary to introduce criteria limiting the subjective and objective circle, determining the time of data retention and a system of domestic remedies that will allow a person whose rights have been violated to assert his or her rights before the courts of a given state.

When analysing the jurisprudence of the ECtHR and the CJEU, one can see a difference in the approach to the protection of individual privacy in relation to the collection of location data. Firstly, the ECtHR assesses whether, in a specific case, the investigative measures applied had a proper basis in national law, were proportionate and necessary in a democratic society. As a general rule, it does not assess the laws of the Council of Europe states in general. It reacts post factum to flawed action by state authorities. The CJEU, on the other hand, examines national



legislation in isolation from the circumstances of the particular case. It checks whether the adopted solutions can be reconciled with EU law (and the EU level of protection of fundamental rights).

Secondly, the lengthiness of the ECtHR proceedings means that the decisions concerning the collection of location data are inadequate to the current technological possibilities. The Strasbourg Court has not yet addressed the issue of automatic processing and collection of data in real time, and thus has not determined under what conditions such information obtained may be used in a criminal trial. For this reason, among others, the CJEU is in a better position to develop coherent, European (EU) rules for the collection and processing of location data in the future. The case law of the Luxembourg court also has the advantage of pointing in the right direction and suggesting to EU countries how they should amend their national laws.

A major challenge to the protection of individual privacy is the problem of mass and automated collection of location data<sup>101</sup>. In order to protect national security, in the *La Quadre du net* judgment, the CJEU allowed for this, provided that the data are individualised and analysed in a traditional (non-automated) way before being used in criminal proceedings. Also the ECtHR - if criteria are specified in national law - allows for the bulk collection of data on an individual<sup>102</sup>.

To sum up, it seems that the European Courts are trying to create a harmonised (or at least inconsistent) standard of protection of the right to privacy in relation to the collection of location data for the purpose of preventing and combating serious crime. The ECtHR does not try to

---

<sup>101</sup> The problem of bulk collection of data on an individual was also the subject of Opinion 1/15 on the draft agreement between Canada and the European Union on the transfer and processing of passenger name records. Advocate General Paolo Mengozzi refers, inter alia, to the problem of automated data processing (see paragraph 252). The position presented in this opinion is in line with that of the Judgment of *La Quadre du Net*, although the issue addressed in that judgment concerned location data. See: OPINION OF ADVOCATE GENERAL Paolo Mengozzi, delivered on 8 September 2016, opinion 1/15; <http://curia.europa.eu/>.

<sup>102</sup> See: EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 10 July 2019, Big Brother Watch and the Others v the United Kingdom*, case no. 58170/13, <https://hudoc.echr.coe.int/>

interfere with the competences of the CJEU, and the CJEU - in creating an EU model of protection of the right to privacy - is based on the case law of the ECtHR. The case law of the ECtHR is late in relation to the developing technological possibilities, but the existing Strasbourg acquis, the general conditions for interference with the right to privacy, provides a good basis for the CJEU to create a model within the EU which, on the one hand, will protect the public against serious crime and, on the other hand, will not lead to a disproportionate interference with individual freedoms and rights.

## BIBLIOGRAPHY

BREYER, Patric. Telecommunication Data Retention. *European Law Journal*, v. 11, no. 3, 2005. <https://doi.org/10.1111/j.1468-0386.2005.00264.x>

BU-PASHA, Shakila, ALEN-SAVIKKO, Anette, MEIKINEN, Jenna, GUINNESS, Robert, KORPISAAR, Päivi. EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency. *European Data Protection Law Review* vol. 2, no. 3, 2016; <https://doi.org/10.21552/EDPL/2016/3/7>

CELESTE, Edoardo. The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios. *European Constitutional Law Review*, v. 15, 2019; <https://doi.org/10.1017/S1574019619000038>

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, published in the Official Journal of the European Union no. C 326/391 on 26 October 2012. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

COUNCIL FRAMEWORK DECISION 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking; published in the Official Journal of the European Union no. L 335/8 of 25 October 2004, <https://eur-lex.europa.eu/>

COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment (Grand Chamber) of 6 October 2020*. C-511/18, C-512/18, C-520/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net (hereinafter: La Quadrature du Net and the others). <http://curia.europa.eu/>

COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 2 October 2018, Ministerio Fiscal*, C-207/16, <http://curia.europa.eu/>

COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 21 December 2016, Tele2 and Watson*, C-203/15 and C-698/15, <http://curia.europa.eu/>

COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 6 October 2020, Privacy International*, C-623/17, <http://curia.europa.eu/>

COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment of 8 April 2020, Digital Rights Ireland*, C-293/12 and C-594/12, <http://curia.europa.eu/>

DIRECTIVE (EU) 2011/36 of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, published in the Official Journal of the European Union no. L 101/1 of April 2011, <https://eur-lex.europa.eu/>

DIRECTIVE (EU) 2011/92 of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA published in the Official Journal of the European Union no. L 335/1 of 17 December 2011, <https://eur-lex.europa.eu/>

DIRECTIVE (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, published in the Official Journal of the European Union no. L 141/73 of 5 June 2015; <https://eur-lex.europa.eu/>

DIRECTIVE (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; The Official Journal of the European Union no. L 119/89 on 4 April 2016; <https://eur-lex.europa.eu/>

DIRECTIVE 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); The Official Journal of the European Union no. L 201/37 on 31 July 2002; <https://eur-lex.europa.eu/>

DOCKSEY, Christopher, HIJMANS, Hielke, The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the

Start of a New Era of Data Protection Law. *European Data Protection Law Review* (EDPL), vol. 5, no. 3, 2019. <https://doi.org/10.21552/edpl/2019/3/6>

DOCKSEY, Christopher. Ministerio Fiscal: Holding the line on ePrivacy. *Maas-tricht Journal of European and Comparative Law*, vol. 26, no. 4, p. 585–594, 2019; <https://doi.org/10.1177/1023263X19853714>

EUROPEAN CONVENTION OF HUMAN RIGHTS, adopted in Rome on 4 November 1950. Available at: [https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf)

EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 12 May 2020, Ringler v Austria*, case no. 2309/10, <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Decision of 29 September 2020, Tretter and the others v Austria*, case no. 3599/10, <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 10 July 2019, Big Brother Watch and the Others v the United Kingdom*, case no. 58170/13, <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 1 March 2007, Heglas v the Czech Republic*, case no. 5935/02, <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 12 January 2016, Szabó and Vissy v Hungary*, case no. 37138/14; <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 2 September 2010, Uzun v Germany*, case no. 35623/05; <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 4 December 2015, Roman Zakharov v Rosji*, case no. 47143/06. <https://hudoc.echr.coe.int/>.

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 December 2009, Previti v Italy*, case no. 45291/06, <https://hudoc.echr.coe.int/>

EUROPEAN COURT OF HUMAN RIGHTS. *Judgment of 8 February 2018, Ben Faiza v France*, case no. 31446/12. <https://hudoc.echr.coe.int/>.

GARLICKI, Lech in: GARLICKI, Lech, HOFMAŃSKI, Piotr. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa 2011

JASIŃSKI, Wojciech, The limits of interference with the right to liberty, privacy property and privilege against self-incrimination in criminal proceedings – European standards, in: SKORUPKA, Jerzy (ed.), *The Model of Acceptable Interference with the Rights and Freedoms of a Individual in the Criminal Process*, Warsaw 2017.

MURPHY, Maria Helen. Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger. *Irish Criminal Law Journal* t. 105, v. 24, no. 4, 2014

OJANEN, Tuomas. Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, *European Constitutional Law Review*, v. 10, no. 3; <https://doi.org/10.1017/S1574019614001345>

OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona delivered on 15 January 2020, C-623/17, Privacy International. <http://curia.europa.eu/>

OPINION OF ADVOCATE GENERAL Campos Sanchez-Bordona, delivered on 15 January 2020, case no. C-520/18; <http://curia.europa.eu/>

OPINION OF ADVOCATE GENERAL Paolo Mengozzi, delivered on 8 September 2016, opinion 1/15; <http://curia.europa.eu/>

REGULATION (EU) 2016/679 of European Parliament and 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; published in the Official Journal of the European Union no. L 119/1 of 4 May 2016; <https://eur-lex.europa.eu/>

STACHNIK-ROGALSKA, Agnieszka; ROGALSKI Maciej. Udostępnianie billingów rozmów telefonicznych. *Państwo i Prawo* no. 8.

STEIN Shlomit, In Search of 'Red Lines' in the Jurisprudence of the ECtHR on Fair Trial Rights. *Israel Law Review* v. 50, no. 2, 2017. <https://doi.org/10.1017/S0021223717000073>

THE TREATY ON EUROPEAN UNION; consolidate version published in the Official Journal no C 326 on 26 October 2012. <https://eur-lex.europa.eu/>.

THIERSE, Stephen. The Never-Ending Story of Data Retention in the EU, [in:] THEIERSE, Stephen, BADANJAK, Sanja. Opposition in the EU Multi-Level Polity. Legal Mobilization against the Data Retention Directive. Springer 2020, <https://doi.org/10.1007/978-3-030-47162-0>

ZUBIK, Marek, PODKOWIK, Jan, RYBSKI, Robert. Prywatność. Wolność u progu D-day. *Gdańskie Studia Prawnicze*, t. XL, p. 391-408, 2018, [https://czasopisma.bg.ug.edu.pl/index.php/gdanske\\_studia\\_prawnicze/article/view/3501](https://czasopisma.bg.ug.edu.pl/index.php/gdanske_studia_prawnicze/article/view/3501)

### **Additional information and author's declarations (scientific integrity)**

*Acknowledgement:* This work is a result of the research project financed by the Polish National Science Center 2017/27/B/HS5/00854.

*Conflict of interest declaration:* the author confirms that there are no conflicts of interest in conducting this research and writing this article.

*Declaration of authorship:* all and only researchers who comply the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

*Declaration of originality:* the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; he also attests that there is no third party plagiarism or self-plagiarism.

### **Editorial process information**

(<http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies>)

- Submission date: 21/12/2020
- Preliminary control and similarity verification: 04/01/2021
- Review 1: 10/01/2021
- Review 2: 10/01/2021
- Review 3: 04/02/2021
- Editorial decision 1: 04/02/2021
- Correction round return: 18/02/2021
- Final editorial decision: 19/02/2021

### **Editorial team responsible**

- Editor-in-chief: 1 (VGV)
- Associated-editor: 1 (KK)
- Reviewers: 3