The role of constitutional courts in taming adverse impact of new technologies in the criminal proceedings

O papel das cortes constitucionais em reduzir os impactos negativos das novas tecnologias no processo penal

Michalina Marcia[1]
University of Wrocław, Poland
michalina.marcia@uwr.edu.pl
https://orcid.org/0000-0002-7872-8507

Abstract: This article presents the impact of constitutional courts in shaping the fair trial standards in the context of new technologies application in the criminal proceedings. Surveillance measures based on the use of new technologies by law enforcement agencies are highly intrusive in nature and may violate not only the constitutional right to privacy, but also, in the author's opinion, guarantees of the fair trial and procedural rights of the suspect. The aim of the article is to indicate to what extent constitutional courts have contributed to establishing the procedural standards in the activities of gathering evidence using new technologies (regarding both content and metadata), as well as to present potential problems in this area that courts will have to face in the future.

Keywords: New technologies; constitutional courts; data retention; surveillance.

Resumo: *Este artigo apresenta os impactos das cortes constitucionais em modelar os parâmetros do devido processo no contexto da aplicação das novas tecnologias no processo penal. Medidas de vigilância baseadas no uso de novas tecnologias*

[1] PhD student at the Chair of Constitutional Law (Faculty of Law, Administration and Economics, University of Wroclaw), Research Assistant at the Digital Justice Center.

pelas agências de persecução são altamente intrusivos em essência e podem violar não somente o direito constitucional à privacidade, mas também, na visão da autora, garantias do devido processo e direitos processuais do suspeito. O objetivo deste artigo é indicar qual a extensão da contribuição das cortes constitucionais para o estabelecimento de critérios processuais nas atividades de obtenção de provas por meio de novas tecnologias (em relação tanto ao conteúdo quanto à metadata), assim como apresentar os potenciais problemas nesse tema, os quais deverão ser enfrentados pelas cortes no futuro.

Palavras-chave: *novas tecnologias; cortes constitucionais; conservação de dados; vigilância.*

1. Introduction

The use of new technologies in criminal proceedings has undoubtedly been gaining in importance recently. Avoiding facing them in the practice of applying the law is, in fact, significantly hindered. This is the result of their widespread use in society[2], but also their prevalence

[2] In 2020 in Poland the use of fixed-line Internet access per households amounted to 56.7%. Dedicated mobile access via modems, cards and keys was used by 23.5% of the population, Possibility of access to the Internet at a speed of min. 75.9% of households have 30 Mb / s; 141, 5% of mobile network. OFFICE OF ELECTRONIC COMMUNICATION. Report of June 2021, https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/391/10/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2020_roku_.pdf (access: January 9, 2022). Also, 95% of American adults own a cell phone, while 77% own a smartphone. *See* PEW RESEARCH CENTER FO INTERNET AND TECHNOLOGY. Mobile Fact Sheet, Pew Research Center for Internet and Technology of February 5, 2018, https://www.pewinternet.org/fact-sheet/ mobile/. According to one of the polls, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, RANGAVIZ, David, Compelled decryption & state constitutional

in operational practice of law enforcement agencies, which must adapt their apparatus to contemporary technological challenges and ensure the effectiveness of their activities.

However, the issue of adapting legal solutions to the current problems of the applying the law raises many doubts. It seems that a large part of the legislations of individual countries reacts to the existing problematic issues with some delay and the process of regulating issues related to the use of new technologies in criminal proceedings takes place only after some time of their practical application, in particular with regard to the implementation of relevant procedural rights of parties to the proceedings. In such a state of facts, the courts are often responsible for clarifying the shape of these powers in a way that goes further than in the case of traditional procedural institutions, and thus for the level of ensuring the standards of a fair trial. This process also takes place at the level of district and local courts, however, due to their specific role and nature, it is the constitutional courts that have a particularly strong impact on the identification of the limits of procedural rights, which not only relate to individual cases, but also shape the general content of the rights making up a concept of the fair trial.[3]

The research question of the study is as follows – do the constitutional courts have a role in shaping the fair trial standards in criminal proceedings with regard to the use of new technologies. The research is based on the European continental system with the particular focus on Polish legal order and Polish Constitutional Tribunal Case Law. Although the author does not undermine its importance, the case law of Polish Supreme Court, administrative, district and local courts were excluded due to the scope of this particular study. To provide for

protection against self-incrimination. *American Criminal Law Review*, v. 57, no. 1, p. 157-206, 2020.

[3] Sometimes, due to the lack of proper regulation and basis for particular measures, the courts also declare some provisions unconstitutional. E.g. in Spain Constitutional Court considered unconstitutional recording of conversations through a hidden device installed in the inmates' prison cells because of the lack of a sufficient legal grounds. BACHMAIER WINTER, Lorena. Remote computer searches under Spanish Law: The proportionality principle and the protection of privacy. *Zeitschrift für die gesamte Strafrechtswissenschaft,* v. 129 no. 1, p. 205-231, 2017. https://doi.org/10.1515/zstw-2017-0008

adequate legal frames the study also analyzes the CJEU and ECtHR case law connected with the discussed problems. In the part dedicated to the privilege against self-incrimination author additionally includes the case law of the Supreme Court of the United States to reflect on issues that have not yet met with the sufficient recognition among European courts. In the legal traditions of the US and Commonwealth countries, derived from the common law system, there are no constitutional courts, while problems related to ensuring respect for procedural rights are resolved by supreme courts and lower instance courts.[4] The example of the United States and problematic issues settled by the Supreme Court regarding the US Constitution and its amendments, in particular the Fifth, is, however, a perfect example of what challenges will constitutional courts face in the future, what will be presented in the further part of the article.

The study is focused mainly on the surveillance measures used by the law enforcement agencies (LEAs) applying to both content and non-content data and on the pre-trial phase of proceedings. In author's opinion it is the stage, in which, especially in case of Polish legal system, the right to a fair trial is especially vulnerable to infringement. One of the main hypothesis of the study is that right to a fair trial and right to privacy in the analyzed scope have some common elements and judgments addressing the problem of right to privacy can also affect the fair trial standard. In the existing Polish case law it can be observed that Constitutional Tribunal rarely addresses directly fair trial standards in regard to legislation regulating the use of new technologies during the proceedings. The author however claims, that constitutional courts influence fairness of the proceedings not only by shaping the content of fair trial *per se*, but also creating fundamental standards for other constitutional rights that ultimately affect the individual procedural rights during the trial.

---

[4] DIXON, Rosalind. Updating Constitutional Rules. *The Supreme Court Review*, no. 1, p. 319–346, 2009. https://doi.org/10.1086/653651, CHOPRA, Pran. The Constitution and Supreme Court. *Economic and Political Weekly*, *v. 39* no. 30, p. 3355–3359, 2004. http://www.jstor.org/stable/4415313, DEENER, David. Judicial Review in Modern Constitutional Systems. *The American Political Science Review*, v. 46 no, 4, 1079–1099, 1952. https://doi.org/10.2307/1952114

The article is structured as follows. First of all it addresses the common aspects of the right to a fair trial and right to privacy to provide a point of reference to further analysis. In the next part it discusses the case law referring to problems connected with gathering digital evidence with distinction between non-content and content data. In the part regarding to non-content data the study is focused on data retention due to the fact that it became the particular interest of constitutional courts in the EU and therefore is of much importance to the research. Then, the article presents the emerging problems for the European constitutional courts connected with the privilege against self-incrimination that have not been yet widely addressed among particular countries. Finally, the study provides for general and fundamental conclusions that can contribute to answering the main research question.

2. Fair trial and right to privacy

As a rule, the problems caused by the dissemination of new technologies in the criminal proceedings are most often identified with the right to privacy, and it is the sphere that the judicial decisions of not only constitutional courts, but also, among others, European Court of Human Rights, refer to.[5] This is understandable, as new technologies inherently have the potential to be highly intrusive, so the general protection model here has been grounded in the content of the right to privacy. It should be noted, however, that the case law in this area also has a huge impact on the implementation of rights resulting from the right to a fair trial.[6]

---

[5] EUROPEAN COURT OF HUMAN RIGHTS (Hereinafter as "ECtHR"). Judgments in cases: S. and Marper v. the United Kingdom 4 December 2008 (Grand Chamber), B.B. v. France (no. 5335/06), Gardel v. France and M.B. v. France (no. 22115/06) 17 December 2009, Shimovolos v. Russia 21 June 2011, Robathin v. Austria 3 July 2012, M.K. v. France (no. 19522/09) 18 April 2013, Brunet v. France 18 September 2014, Szabó and Vissy v. Hungary 12 January 2016, Trabajo Rueda v. Spain 30 May 2017, Aycaguer v. France 22 June 2017, Gaughran v. the United Kingdom 13 February 2020, Centrum För Rättvisa v. Sweden 25 May 2021 (judgment – Grand Chamber).

[6] About right to a fair trial see also: HARRIS, David. The right to a fair trial in criminal proceedings as a human right, *International & Comparative Law Quarterly*, v. 16 n. 2, p. 352-378, 1967, https://doi.org/10.1093/

The elements and specific institutions distinguished under both of these rights, i.e. the right to privacy and the right to a fair trial, are to a large extent interrelated and affect the mutual implementation of standards for the protection of constitutional rights.

One such institution is undoubtedly the right to notification. The right to notification, mentioned primarily in the scope of the right to the protection of personal data, is an integral part of the right to active participation in the proceedings, which is an element of the right of defense.[7] Without informing the suspect or accused about the activities carried out against him, even if such information is delayed in time, they*de facto* loses the possibility of effective defense, taking any action in relation to the measures applied by law enforcement agencies, including questioning their legality and proportionality. The latter is also associated with the right to judicial review, especially of particularly intrusive measures, which appears often in the case law.[8] Enabling the suspect the access to judicial control of actions taken against him not only strengthens the protection of their right to privacy, but also largely protects the overall fairness of the proceedings.

It should also be noted that in the case of activities involving the use of digital evidence, due to their nature, the suspect is often completely

---

iclqaj/16.2.352, VITKAUSAS, Dovydas; DIKOV, Grigoriy. *Protecting the right to a fair trial under the European Convention on Human Rights. Council of Europe*, Available at: https://edoc.coe.int/en/module/ec_addformat/download?cle=c82b013313066e0702d58dc70db033ca&k=2fc0fa200f64659df501f62a8386baad. Accessed: March 23, 2022, BREMS, Eva. Conflicting human rights: an exploration in the context of the right to a fair trial in the European Convention for the protection of human rights and fundamental freedoms. *Human Rights Quarterly*, v. 27, n. 1, p. 294-326, 2005, https://doi.org/10.1353/hrq.2005.0003 , MAHONEY, Paul. Right to a fair trial in criminal matters under Article 6 ECHR. *Judicial Studies Institute Journal*, v. 4, n. 2, p. 107-129, 2004, AKTHER, Shajeda; NORDIN, Rohaida. An Analysis of Fair Trial Guarantees at Trial Stage under the ECHR, *Law Review* p. 211-234, 2015.

7 WILIŃSKI, Paweł. *Proces karny w świetle Konstytucji*, Warsaw: Wolters Kluwer Polska, p. 174-177, 2011, LACH, Arkadiusz. *Rzetelne postępowanie dowodowe w sprawach karnych w świetle orzecznictwa strasburskiego*, Warsaw: Wolters Kluwer Polska, p. 112-158, 2019, CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of May, 17 2004, SK 32/03 OTK-A no. 5, p. 44.

8 CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of December, 12 2005 r., K 32/04.

unaware of the surveillance carried out against him, therefore it is not possible to take any action or legal remedies in the criminal proceedings related to the measures used by law enforcement authorities. The grounds for justifying the lack or delay of information are generally connected with the sake of the proceedings and eliminating the potential obstruction of the trial.[9] In this case, at the constitutional level, it is a premise of security and public order, and from the criminal trial perspective, it is an attempt to deliver an effective, just ruling and implement the appropriate criminal response. However, the problem arises as to whether such a far-reaching restriction can be considered proportionate.[10]

The principle of proportionality is also extremely important to the fairness of the proceedings. It is an element of the European human rights standard, although it is often not directly expressed in legal acts.[11] It is considered to be the necessary element of the legal systems based on the rule of law and democratic principles.[12] The proportionality test, based on the adequacy, necessity and proportionality *stricto sensu* became a part of constitutional traditions of particular states as a result of

---

[9] OLBER, Paweł. Remote Search of IT System in Polish Legislation and Its Importance in Fight Against Cybercrime, *Internal Security*, v. 11, n. 2, p. 141-140. http://dx.doi.org/10.5604/01.3001.0013.8288. See also LOFTUS, Bethan. Normalizing covert surveillance: the subterranean world of policing, *The British Journal of Sociology*, p. 2070-2091, https://doi.org/10.1111/1468-4446.12651

[10] The right to notification is a problematic issue not only at the national level, but also raises doubts in the context of EU legal solutions. It is one of the main points of contention connected with the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD). EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. Opinion EESC 2018/02737, OJ C 367, 10.10.2018, p. 88–92. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11314_2021_INIT&from=EN>. Accessed: January 9, 2022.

[11] The exception can be the Charter of Fundamental Rights of the European Union. ŚLEDZIŃSKA SIMON, Anna. *Analiza proporcjonalności ograniczeń konstytucyjnych praw i wolności. Teoria i praktyka*, p. 24, 2019. https://doi.org/10.34616/23.19.020

[12] BARAK, Aharon. *Proportionality. Constitutional Rights and Their Limitations*, Cambridge: Cambridge University Press, p. 472, 2006.

"judicial borrowing"[13]. Now it is said to be the common judicial standard of European constitutional courts and European Court of Human Rights as well.[14] It has frequently been also the subject of Constitutional Tribunal of Poland case law.[15]

When addressing the impact of new technologies on human rights standards, Constitutional courts, including the Constitutional Tribunal of Poland, often raise the problem of proportionality in the context of restricting the constitutional right to privacy.[16] However, at the same

---

[13] CHOUDHRY, Sujit (ed.). *The Migration of Constitutional Ideals*, Cambridge: Cambridge University Press, 2006, JACKSON, Vicki. *Constitutional Engagement in a Transnational Era*, Oxford: Oxford University Press, p. 60, 2010, KUMM, Mattias. Constitutional Rights as Principles, *International Journal of Constitutional Law* v. 2, p. 595, 2004, https://doi.org/10.1093/icon/2.3.574, BARKHUYSEN, Tom, EMMERIK, VAN, Michiel, JANSEN, Oswald, FEDOROVA, Masha. Right to a Fair Trial. In: DIJK, VAN, Pieter, HOOF, Van, Fried RIJN, VAN, Arjen, ZWAAK, Leo. *Theory and practice of the European Convention on Human Rights*, Cambridge: Intesentia, p. 637, 2018.

[14] BARAK, 181–206, J. McBride, Proportionality and the European Convention of Human Rights, [w:] E. Ellis (red.), The Principle of Proportionality in the Laws of Europe, Portland 1999, s. 23

[15] CONSTITUTIONAL TRIBUNAL OF POLAND. Judgments of 11 February 1992 r., K 14/91, 26 January 1993, U 10/92, 17 October 1995, K 10/95, 25 November 2003, K 37/02, 9 July 2009, SK 48/05, 25 July 2013, P 56/11, 5 June 2014 r., K 35/11, 14 July 2015, SK 26/14, 4 November 2015, K 1/14, WÓJTOWICZ, Krzysztof. Zasada proporcjonalności jako wyznacznik konstytucyjności norm. In: ZUBIK, Marek (ed.). *Księga XX-lecia orzecznictwa Trybunału Konstytucyjnego*, Warsaw: Biuro Trybunału Konstytucyjnego, 265– 278, 2006, GARLICKI, Lech; WOJTYCZEK, Krzysztof. Komentarz do art. 31 Konstytucji. In: GARLICKI, Lech; ZUBIK, Marek (ed.). *Konstytucja Rzeczypospolitej Polskiej*. Komentarz, t. II, Warsaw: Wolters Kluwer Polska, p. 69, 2016, TULEJA, Piotr. Komentarz do art. 31 Konstytucji. In: TULEJA, Piotr (ed.). *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warsaw: Wolters Kluwer Polska, p. 114.119, 2019, BANASZAK, Bogusław. *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa: C.H.Beck, p. 212, 2012.

[16] ROJSZCZAK, Marcin. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. *European Constitutional Law Review*, p. 1-29, 2021. doi:10.1017/S157401962100035, see also *i.a.* FEDERAL CONSTITUTIONAL COURT, Press release no 11/2010 of 2 March 2010. DE VRIES, Katja, BELLANOVA Rocco, DE HERT Paul, GUTWIRTH Serge. The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?). In: GUTWIRTH Serge, POULLET Yves, DE HERT Paul, LEENES Ronald

time, the existing case law ensures the proportionality of all measures taken against the suspect or accused in the proceedings, thus ensuring that the standards of a fair trial are met.

One of the main rules of a fair trial, which can be found in the case law of constitutional courts, is the principle of equality of the parties, related in particular to the adversarial model of the trial. This principle assumes no clearly dominant procedural position of any of the parties and its implementation undoubtedly contributes to ensuring the right of defense.[17] It should be noted, however, that due to the fact that law enforcement agencies have a wide range of resources and the entire state apparatus at their disposal, this principle can never be fully implemented in practice. This is particularly evident in the use of new technologies, where the data acquisition rights are often one-sided.[18] Respecting the requirement of proportionality in the application of measures aimed at interfering with the sphere of privacy of the suspect will therefore also contribute to ensuring equality of the parties. It should be pointed out that in view of the tendency to transfer the center of procedural activity to the first stage of proceedings and the possibility of collecting data in a large amount and on a large scale, this protects the suspect from finding themself in a situation in which they will *de facto* have to prove their innocence and question the standard of presumption of innocence.[19] The principle of proportionality, even if invoked in the context of the right to privacy, is therefore of great importance to the fair trial guarantees.

In connection with the above mentioned arguments, it seems that the strict limitation of the sphere of influence of new technologies on

---

(eds) Computers, Privacy and Data Protection: an Element of Choice, p. 3-23, 2011, https://doi.org/10.1007/978-94-007-0641-5_1

[17] SKRĘTOWICZ, Edward. Z problematyki rzetelnego procesu karnego. In: SKORUPKA, Jerzy (ed,), Rzetelny proces karny. Księga jubileuszowa Profesor Zofi i Świdy, p. 23, 2009, PIECH, Michał Glosa do wyroku TK z dnia 25 września 2012r., SK 28/10.

[18] This applies *i. a.* to the possibility of asking operators directly to provide data, the inability to independently obtain evidentiary material and present evidence.

[19] STOYKOVA, Radina. Digital evidence: Unaddressed threats to fairness and the presumption of innocence, *Computer Law & Security Review*, v. 42, 2021. https://doi.org/10.1016/j.clsr.2021.105575

respect for human rights only to the right to privacy cannot be perceived as justified. Therefore, the question arises, whether the elements of protection of both indicated rights have many common points, or whether, due to the progressive change in the measures applied by law enforcement agencies, excessive restriction of the suspect's right to privacy in the trial will translate into the overall fairness of the proceedings.

Both the European Court of Human Rights and the Court of Justice of the European Union[20] referred to this issue to some extent. The previous case law of the European Court of Human Rights shows that, when referring to use of new technologies, especially surveillance measures, in principle, the Court does not include in its decisions connection between the violation of the right to privacy through the use of specific measures by law enforcement agencies and the right to a fair trial.[21] Despite finding numerous violations of Article 8 of the European Convention on Human Rights[22], in terms of the use of new technologies in the proceedings, it often refused to recognize a violation of Art. 6 of the ECHR, despite the fact that the collected evidence was based on the above-mentioned methods.[23] However, the Court does not clearly preclude that possibility. In the recent judgments, there appear some indications of a link between excessive or unlawful surveillance measures used as a basis for conviction and Article 6 infringement.[24] Nevertheless, at the moment it is difficult to identify an unambiguous line of case law in this respect, and the violation of Article 6 is often combined with other elements and infringed rights as well.

---

[20] Hereinafter also as "CJEU".

[21] Excluding, of course, situations where surveillance measures are applied to conversations between suspect or accused and their defense counsel, which Court finds as a clear breach of article 6 (3) of the Convention. See e.g. EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 16 November 2021, Vasil Vasiliev v. Bulgaria, app. no. 7610/15.

[22] EUROPEAN CONVENTION OF HUMAN RIGHTS, adopted in Rome on 4th November 1950. Available at: https://www.echr.coe.int/documents/con-vention_eng.pdf. (access: January 9, 2022). Hereinafter as the "ECHR".

[23] EUROPEAN COURT OF HUMAN RIGHTS. Press Unit, Factsheet – new technologies, 2021. Available at: https://www.echr.coe.int/documents/fs_new_technologies_eng.pdf. (access: January 9, 2022).

[24] EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 14 October 2021, Lysusk v. Ukraine, app. no. 72531/1.

A slightly different position can be found in the recent case law of the Court of Justice of the European Union. The Court, with regard to the problem of *i.a.* data retention, has indicated that the final evidential use of materials obtained through disproportionate and illegal electronic evidence gathering has a particular impact on the respect of the standard to a fair trial. The Court pointed out, that the need to exclude information and evidence obtained in breach of Union law must be assessed, in particular, in the light of the risk which the admissibility of such information and evidence presents to respect for the adversarial principle and thus the right to a fair trial. Therefore, in the Court's view, the principle of effectiveness imposes an obligation on the national criminal courts to disregard information and evidence obtained through measures incompatible with EU in the framework of criminal proceedings instituted against persons suspected of committing a crime, if these persons are not able to effectively respond to the information and evidence belonging to an area not examined by the court and which may have a decisive influence on the assessment of the facts. According to CJEU, otherwise the State would admit to some extent the possibility of violating the right to a fair trial by failing to ensure the right to active participation in the trial.[25]

Taking into account the above mentioned elements, it, therefore, seems that the role in shaping the fair trial standards will have not only judicial decisions addressing the fair trial directly, but to some extent also case law that refer to right to privacy infringements.

3. Data retention

Undoubtedly, a notable influence of constitutional courts on respecting the procedural rights of participants in proceedings can be observed in the context of data retention. The issue of retention is most often identified with the right to privacy and the right to the protection of

[25] Judgment (Grand Chamber), 2 March 2021, C-746/18, *Criminal proceedings against H. K.,* EU:C:2021:152, judgment of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Other*s, joined cases C-511/18, C-512/18 i C-520/18, EU:C:2020:791, p. 226, 227.

personal data, in particular.[26] The method of using the evidence obtained in this way is, however, not without significance also for the observance of the rules of the fair trial during the criminal proceedings.

Data retention itself is generally defined as an obligation imposed on telecommunications operators (service providers) to collect and store information about connections made within the mobile network and the Internet.[27] The Directive 2006/24/EC adopted in 2006[28], imposed an obligation on member States of EU to retain and store particular categories of 'data by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of

---

[26] MITROU, Lilian. The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive. In HAGGERTY, Kevin, SAMATAS, Minas Samatas (eds). *Surveillance and Democracy*, New York: Routledge, 2010, TAYLOR, Mark. The EU Data Retention Directive *Computer Law & Security Review,* v. 22 p. 309-312, 2006. https://doi.org/10.1016/j.clsr.2006.05.005; MARAS, Marie-Helen. From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?. In GOOLD, Benjamin J., NEYLAND, Daniel (eds). *New Directions in Surveillance and Privacy*, Willan, 2009. https://doi.org/10.4324/9781843927266, JUSZCZAK, Adam, SASON, Elisa. Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning? *EUCRIM* v. 4, p. 238 – 266, 2021, CZERNIAK, Dominika. Collection of location data in criminal proceedings – European (the EU and Strasbourg) standards. *Revista Brasileira de Direito Processual Penal*, v. 7, n. 1, p. 123-160, 2021. https://doi.org/10.22197/rbdpp.v7i1.503, VERBRUGGEN, Frank; CONINGS, Charlotte. After zigzagging between extremes, finally common sense? Will Belgium return to reasonable rules on illegally obtained evidence? *Revista Brasileira de Direito Processual Pena*l, v. 7, n. 1, p. 273-310, 2021. https://doi.org/10.22197/rbdpp.v7i1.500

[27] FUNDACJA PANOPTYKON, Telefoniczna Kopalnia Informacji. Przewodnik, p. 20. Available at: http://panoptykon. org/biblio/telefoniczna–kopalnia–informacji–przewodnik. (access: January 9, 2022).

[28] DIRECTIVE 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, Available at: http://data.europa.eu/eli/dir/2006/24/oj. Declared invalid by the judgment of 8 April 2014, joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

the Member State in the process of supplying the communication services concerned'. The act and new national regulations created, however, such controversy in some of the countries, that the issue had to be addressed by constitutional courts.[29]

In this case, constitutional courts adopted more protective position in relation to the constitutionally guaranteed fundamental rights. In many member States there appeared judgments stating that data retention regulated in such way as in the directive is unconstitutional and irreconcilable with constitutional rights and freedoms guaranteed in particular countries.[30] The rendered judgments influenced not only local concepts of procedural rules and fairness, but also general European standards[31].

The constitutional courts generally questioned not the retention *per se*, but procedural guarantees that were lacking in the resolutions of the Directive. First of all, the courts found problematic general lack of precision within the regulation which led to questioning the legal security and even presumption of innocence.[32] In many countries' laws implementing the Directive provisions there were no clear indication of the type of data subjected to the retention and authorities competent to

---

[29] VAINIO, Niklas, MIETTINEN, Samuli. Telecommunications data retention after Digital Rights Ireland*:* legislative and judicial reactions in the Member States, *International Journal of Law and Information Technology*, v. 23, no. 3, p. 290–309, 2015. https://doi.org/10.1093/ijlit/eav010

[30] BULGARIAN SUPREME ADMINISTRATIVE COURT, Decision No 13627, 11 December 2008, CONSTITUTIONAL COURT OF ROMANIA, Decision No 1258 of 8 October 2009, CONSTITUTIONAL COURT OF THE CZECH REPUBLIC, Decision of 22 March 2011, Pl. ÚS 24/10, decision of 22 December 2011, Pl. ÚS 24/11.

[31] ZUBIK, Marek; PODKOWIK, Jan; RYBSKI, Robert. *European Constitutional Courts towards Data Retention Laws*, Cham: Springer, 2021, https://doi.org/10.1007/978-3-030-57189-4

[32] CONSTITUTIONAL COURT OF ROMANIA, Decision No 1258 of 8 October 2009, FEDERAL CONSTITUTIONAL COURT, Press release no 11/2010 of 2 March 2010, CONSTITUTIONAL COURT OF THE CZECH REPUBLIC, Decision of 22 March 2011, Pl. U´ S 24/10' (2012). More about issues connected with presumption of innocecne connected with new technologies application in the proceedings – STOYKOWA, (2021), Digital evidence: Unaddressed threats to fairness and the presumption of innocence, Computer Law & Security Review, Volume 42, https://doi.org/10.1016/j.clsr.2021.105575

collect it.[33] Courts also found that there exist some serious doubts with regard to proportionality.[34] The issue of proportionality was connected not only with the scale of data retention but also with no time limits of applying the measure. The other basic concern of the courts was lack of the adequate control of using the retained data in the criminal trial and the retention process as such. For example Polish Constitution Tribunal stated that there is a need for judicial control to ensure procedural fairness and respect for privacy.[35] The decision of Constitutional Tribunal of Poland addressing data retention (K 23/11)[36] is in fact a perfect example of a case, when despite the fact that the right to privacy was invoked as a point of reference, it was the right to a fair trial that has been affected due to the final decision of the Court. After the judgment in which Court declared the previous regulations incompatible with constitutional right to privacy, Polish legislator introduced in the Act on the Police[37] Article 20ca, in which some type of judicial review was introduced. According to the provisions of the Article, competent authorities every six months submit a report to the circuit court covering the number of cases of obtaining telecommunications, postal or internet data in the reporting period, the type of such data and legal classification of offences in relation to which telecommunications, postal or internet data has been requested, or information on obtaining data in order to save human life or health or to support search or rescue activities. In addition, the circuit court may request materials that justify the disclosure of data to the Police. Although the review in its present shape is said to be insufficient and cannot be

---

[33] CONSTITUTIONAL COURT OF THE CZECH REPUBLIC, Decision of 22 March 2011, Pl. ÚS 24/10, decision of 22December 2011, Pl. ÚS 24/11.

[34] FEDERAL CONSTITUTIONAL COURT, Press release no 11/2010 of 2 March 2010.

[35] CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of December 12, 2005, K 23/04. The Court in its ruling stated that lack of the obligation to obtain consent to covert acquisition of information (surveillance) leads to violation of the fair trial. Similarly, EUROPEAN COURT OF HUMAN RIGHTS. Judgments of 29 June 2006, Weber and Saravia v. Germany, (app. no. 54934/00); 2 Sptember 2010 Uzun v. Germany (app. no. 35623/05).

[36] CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of April 30, 2014, K 23/11.

[37] ACT ON THE POLICE of 6 April 1990, *Dziennik Ustaw,* item 1882.

seen as a proper procedural guarantee compatible with requirements set out by the CJEU[38], its introduction definitely affected the right to a fair trial to some extent.

There appeared also some references to the process of treating the evidence gathered by means of data retention as the base for rendering judgments and potential conviction. According to some of the statements, the final indication of the fact if the trial can be considered fair will be whether the evidence base on unlawful data retention will be used in the proceedings.[39]

The impact of using the evidence collected by means of data retention on the observance of the fair, adversarial trial standards was also noted by the Court of Justice of the European Union in its judgments, as it was already indicated above.[40] However, one of the research conducted by Eurojust shows considerable uncertainty related to the future of admitting evidence obtained through retention inconsistent with the conditions imposed by the CJEU and some of the constitutional courts. While in the Member States, during the EU surveys, the evidence was still generally considered admissible for the purposes of the trial, its future remains uncertain. [41] Therefore, it seems

---

[38] ROJSZCZAK, Marcin. *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warsaw: Wolters Kluwer Polska, 2019.

[39] FEDERAL CONSTITUTIONAL COURT, Judgment of the First Senate of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09.

[40] COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment (Grand Chamber), 2 March 2021, C-746/18, *Criminal proceedings against H. K.*, EU:C:2021:152, judgment of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, joined cases C-511/18, C-512/18 i C-520/18, EU:C:2020:791, See also judgment of 21 December 2016, joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, EU:C:2016:970, judgment of 6 October 2020, Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, EU:C:2020:790.

[41] Five countries reported on court rulings where the admissibility of evidence from data retention was evaluated by the court. So far the evidence has been deemed admissible by courts, although one of the five cases (in Ireland) is still pending on appeal. EUROJUST. Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15

that the creation of compliant, coherent rules regarding the regulation of new technologies in criminal proceedings, e.g. on the basis of the already functioning case law of constitutional courts, will contribute not only to ensuring respect for the fairness of the trial, but also to guaranteeing the effectiveness of the trial.

4. Interception of communications content

Data retention is generally based on metadata, excluding the possibility of intercepting the actual content of messages. This matter, however, has been the subject of interest for constitutional courts for quite some time. Jurisprudence mainly focus on wiretapping and phone communications interception. Nevertheless, with the dissemination of Internet use, the role of online surveillance is significantly increasing. This applies not only to mail interception and digital communications surveillance, but also to the use of remote searches.[42] In the process of determining the scope of procedural guarantees and, therefore, fair trial, both courts and scholars base on the same principles.[43]

---

and C-698/15 – Report, 2017. Available at: <https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf> .Accessed January 9, 2022. See also ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? Computer Law & Security Review, v. 41, 2021. https://doi.org/10.1016/j.clsr.2021.105572, JUSZCZAK, Adam, SASON, Elisa. Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning? *EUCRIM* v. 4, p. 238 – 266, 2021, https://doi.org/10.30709/eucrim-2021-020

[42] A remote search may take the form of an extended search (i.e. when, during a search of a traditional nature, it turns out that the data essential for the taking of evidence are contained in another system related to the primary device in such a way that direct access from it is possible, admissible is extending the search to the above-mentioned system) or remote search *sensu stricto* (i.e. collecting data from the target system based on a specific type of remote investigative software).

[43] See e.g. HAGGERTY, Kevin, SAMATAS, Minas Samatas (eds). *Surveillance and Democracy*, New York: Routledge, 2010.

As a rule, courts consider the covert surveillance measures compatible with state constitutions.[44] However, they also set some conditions necessary to consider regulations constitutional and meeting the requirements of the protection of human rights. In the existing jurisprudence there are some common elements of the constitutional tradition regarding approach to measures including surveillance.

First of all, the courts require an examination of whether surveillance has been ordered on the base of precise, objective indications of a crime, not just by general suspicions. The evidence material has to be examined if there exist facts that rationally, in an objective assessment, indicate the probability that some person is involved in a criminal activity and if they can be supported by objective data.[45]

The courts also indicate, that all powers allowing to covertly collect data must satisfy the principle of proportionality. All forms of surveillance must be supported by weighty legal interests, a threat to which must be sufficiently foreseeable. They may, only under limited conditions, extend also to the third parties. There must be also guaranteed some protection of persons subject to professional confidentiality. Generally, the regulation must fulfill conditions of transparency, individual legal protection and adequate supervisory control.

The problem of digital communications surveillance and remote searches *per se* is less frequently tackled by the decisions of courts. However, e.g. German Federal Constitutional Court addressed directly forms of surveillance of technology systems. The court stated that as a rule the state has to ensure confidentiality and integrity of information technology systems. Such breach of privacy must be perceived as an exception and must be 'based on clear indications of a concrete danger to a predominantly important legal interest, a threat to which affects the basis

---

[44] FEDERAL CONSTITUTIONAL COURT. Judgment of the First Senate of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, judgment of the First Senate of 27 February 2008, 1 BvR 370/07, 1 BvR 595/07, CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of December, 12 2005 r., K 32/04, judgment of July, 30 2014, K 23/11.

[45] CONSTITUTIONAL COURT OF SPAIN. Judgment 253/2006 of 11 September 2006, FEDERAL CONSTITUTIONAL COURT. Judgment of the First Senate of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09.

or continued existence of the state or the basis of human existence. The court also indicated that secret infiltration of an information technology system is in principle to be placed under the reservation of a judicial order'. Moreover, due to the highly intrusive nature of the discussed measures, if the state agency is not authorized to obtain information of the contents of Internet communication, acquiring evidence will constitute the encroachment of the Basic Law provisions.[46]

The courts also referred to the problem of subsequent use of the evidence in the proceedings. This matter is closely related to the fair trial standards, as it ultimately determines, whether the proceedings can be considered fair. E.g. Spanish Constitutional Court rendered a judgment in which it put forward a thesis that evidence obtained, directly or indirectly, in violation of fundamental rights or liberties, will have no effect. It will include also an infringement of right to privacy. Therefore, if the evidence will be used as a basis for final court decision in the criminal proceedings, it will in fact influence the ultimate fairness of the trial.[47]

The case law of constitutional courts regarding the means of gathering evidence with the use of new technologies in proceedings should be definitely assessed positively. Courts, through their judicial decisions, identify certain common elements that should be implemented in individual regulations adopted by the legislator in order to meet the standard guaranteed in the constitution. The last position expressed by the Polish Constitutional Tribunal in the judgment of June 30, 2021 is all the more controversial.

An application has been submitted to the Constitutional Tribunal of Poland to review the constitutionality of the provisions on surveillance measures contained in the Police Act[48] to the extent that they do not provide for judicial review of the order of the abovementioned surveillance, as well as its execution, the maximum duration of these measures and, finally, the right to notify the person to whom it was applied about the

---

[46] FEDERAL CONSTITUTIONAL COURT. Judgment of the First Senate of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09,

[47] CONSTITUTIONAL COURT OF SPAIN, decision STC 114/184, BACHMAIER, Lorena, Exclusionary Rules of Evidence in Spain, in: THAMAN, S. (ed.), Truth versus Legality in a Comparative View, Heidelberg, p. 209–234, 2012.

[48] ACT of 6 April 1990 on the Police, Dz. U. of 2021, item 1882.

conduct of the control after its completion.[49] The constitutional standard in this case was to be, first of all, the right to a fair trial and the right to an effective remedy, *i.e.* Articles 45 and 78 of Polish Constitution[50] and the principle of a democratic state governed by the rule of law. However, in the presented case, the Tribunal found that the question referred by the Ombudsman was groundless and that its subject matter exceeded the scope of the Constitutional Tribunal jurisdiction. The Tribunal stated that the legal status covered by the question was in fact a legislative omission, left within the limits of legislative freedom and thus not subject to constitutional control.[51]

However, this position seems highly unjustified, as the issue of infringing constitutionally guaranteed rights cannot be seen as a legislative omission in the sense adopted by the Constitutional Tribunal. In the light of the previous judgments of the Polish Constitutional Tribunal and other constitutional courts, it seems that this is exactly the particular and significant role of constitutional courts - to check whether the legislator has provided for all constitutionally required procedural guarantees, resulting, *i.a.* from the right to a fair trial, the right of defense and, as a result, if the regulation in question is compatible with the constitutional provisions.

5. Self – incrimination and lie-detecting technologies – the emerging problems

The most developed and broad scope of judgments connected with the issue of use of the new technologies in criminal proceedings,

---

[49] OMBUDSMAN. Motion of 4 December 2015 r., II.511.84.2015.KSz, ATTORNEY GENERAL. Motion of 12 November 2015 r., PG VIII TKw 41/14.

[50] THE CONSTITUTION OF THE REPUBLIC OF POLAND of 2nd April 1997, published in *Dziennik Ustaw* No. 78, item 483.

[51] CONSTITUTIONAL TRIBUNAL OF POLAND. Decision of June, 30 2021 r., K32/05. About the controversies concerning the status of Polish Constitutional Court and its influence on surveillance measures see e.g. ROJSZCZAK, Marcin. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. *European Constitutional Law Review*, p. 609, 2021. https://doi.org/10.1017/S157401962100035

with regard to fair trial standards, has been appearing in the legal orders of USA and Commonwealth.[52] These systems, however, did not include the constitutional courts in their traditions and the role of determining the scope of constitutional provisions is left to district, federal and supreme courts.[53] All the issue that were tackled are, nevertheless, the good indication of what is going to be, in the near future, the concern of the constitutional courts. The content of right of defense and fair trial among existing legal systems tend generally to approximate and have similar core.[54] As a result, the problems that the common law systems are facing now, will have to be finally approached by continental systems. Therefore, it appears beneficial to present some problematic aspects connected with the use of new technologies that have already appeared in Supreme Court of the United States case law.

One of the interesting issues that were tackled in the case law of Supreme Court of the United States, was the relation of privilege against self-incrimination and the use of digital evidence in the proceedings. The privilege (*nemo tenetur*) is the element of the right of defense and fair trial, well established in the constitutional traditions of particular countries. ECtHR stated that it is not directly expressed in the Article 6 of the Convention but acknowledged it as a part of fair trial principle.[55]

---

[52] HERRERA, Adam. Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination, *UCLA Law Review,* v. 66 n. 3, p.778-817, 2019, GERSTEIN, Robert. Privacy and self-incrimination. In SCHOEMAN, Ferdinand David (ed.), *Philosophical Dimensions of Privacy:* An Anthology, Cambridge: Cambridge University Press, p. 245-264, 1984. https://doi.org/10.1017/CBO9780511625138.010

[53] CHOPRA, Pran. The Constitution and Supreme Court. *Economic and Political Weekly*, *v. 39* no. 30, p. 3355–3359, 2004. http://www.jstor.org/stable/4415313, DEENER, David. Judicial Review in Modern Constitutional Systems. *The American Political Science Review*, v. 46 no, 4, 1079–1099, 1952. https://doi.org/10.2307/1952114.

[54] HARRIS, David. The Right to a Fair Trial in Criminal Proceedings as a Human Right, *International and Comparative Law Quarterly,* v. 16 n. 2, p. 352-378, 2008, https://doi.org/10.1093/iclqaj/16.2.352

[55] EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 8 February 1996, *John Murray v. the United Kingdom* (app. no. 18731/91) §45, of 29 June 2007, O'Halloran and Francis v. the United Kingdom, (Applications nos. 15809/02 and 25624/02).

As similar matters, concerning the use of new technologies and their impact on the privilege against self-incrimination, begin to appear before European local and district courts[56], it appears that it is only a matter of time when the constitutional courts will have to take a stand on this matter. The main problem in this sphere is connected with the question if the officers of law enforcement agencies or the prosecutor can compel the suspect to provide the password, encryption key or unlock their phone using biometrical means and data.[57] Supreme Court of the United States examined the scope of the Fifth Amendment provisions and, basing its rulings mainly on the previous decisions concerning the division between real and testimonial evidence. Finally, Court introduced guidelines for the following judgments, differentiating *i.a.* between biometrical and alpha-numerical safeguards.[58] The issue also was analyzed by the courts e.g. of UK, Australia. In the given countries, legislator introduced laws allowing to treat not submitting the passwords and encryption keys as an

---

[56] See for example RECHTBANK NOORD-HOLLAND [District Court of North-Holland, the Netherlands]. Judgment of 25 January 2019, NJFS 15/168454-18.

[57] See e.g. GOLDMAN, Kara. Biometric passwords and the privilege against self-incrimination. *Cardozo Arts & Entertainment Law Journal*, v. 33, no. 1, p. 211-236, 2015.

[58] UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN. *United States v. Kirschner,* 823 F. Supp. 2d 665 (E.D. Mich. 2010), UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT. *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011,* 670 F.3d 1335, 1349 (11th Cir. 2012), UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLORADO. *United States v. Fricosu,* 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012), MASSACHUSETTS SUPREME JUDICIAL COURT. *Commonwealth v. Gelfgatt,* 11 N.E.3d 605, 614-15 (Mass. 2014), DISTRICT COURT OF APPEAL OF FLORIDA. *State v. Stahl,* 206 So. 3d 124, 136-37 (Fla. Dist. Ct. App. 2016), UNITED STATES COURT OF APPEAL FOR THE ARMED FORCES. *United States v. Mitchell H, 76* M.J. 413,424-25 & n.5 (C.A.A.F. 2017), UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT. *United States v. Apple MacPro Computer,* 851 F.3d 238, 248 & n.7 (3d Cir. 2017 138 S. Ct. 1988 (2018), UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA. *United States v. Spencer,* No. *17-cr-00259-CRB-1,* 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018), INDIANA COURT OF APPEAL. *Seo v. State, 109* N.E.3d 418, 425-31 (Ind. Ct. App. 2018) *2018* WL 6565988 (Ind. Dec. 6, 2018).

offence punishable even by imprisonment. The regulations were highly controversial and met with very mixed responses.[59]

The district courts, as well as doctrine representatives, are not unanimous, however, in their conclusions and some voices appeared that the privilege against self-incrimination should be reformulated for the purpose of adjusting criminal proceedings to new technological challenges.[60] As a result, the more impact and meaning will have developing the position on this subject by constitutional courts. It will be interesting to observe, if the courts will share coherent view on the matter or if the scope of the principle in question will differ to the significant extent in particular countries. It seems that there will be an intriguing debate on the concept of real evidence and its meaning in the digital era. Not all of the countries have that clear distinction, as in the constitutional system of the USA, but many visibly draw from it and present similar approach.[61] It is necessary in order to enable e.g. acquiring fingerprints, getting access to evidence material of particular type, however nowadays, as the technological progress shifted our perception of the digital sphere, the question appears, if differentiating the extent of the fair trial guarantees, is in this case justified.

The other issue, emerging from the development of new technological accomplishments that is connected with privilege against self-incrimination, is the broadening scope of lie-detecting measures. The problem of measures based on unconscious reactions of the human body as the basis of conviction evidence, e.g. with the use of polygraph

---

[59] ADAM, Lisanne, BARNS, Greg. Digital strip searches in Australia: A threat to the privilege against self-incrimination, *Alternative Law Journal*, V. 45, no. 3, p. 222–227, 2020. https://doi.org/10.1177/1037969x20923073 See *i. a.* also VICTORIAN COURT OF APPEAL, McElroy v The Queen; Wallace v The Queen [2018] VSCA 126, 55 VR 450, QUEENSLAND COURT OF APPEAL, Wassmuth v Commissioner of Police [2018] QCA 290, FEDERAL COURT OF AUSTRALIA, Luppino v Fisher (No 2) [2019] FCA 1100.

[60] See for example REDMAYNE, Mike. Rethinking the Privilege Against Self-Incrimination, *Oxford Journal of Legal Studies*, v. 27, no. 2, p. 209–232, 2007 https://doi.org/10.1093/ojls/gql001, CARNES, Brittany A. Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones, *Loyola Law Review,* v. 66, n.1, p. 183-210, 2020.

[61] WILIŃSKI, Paweł. Zasada prawa do obrony w polskim procesie karnym, p. 354-359, 2006.

was the subject of decisions of constitutional courts in the past. [62] Most constitutional courts of individual states indicated that it is possible to admit evidence from analysis of this type if the accused or the suspect voluntarily submits to them. Currently, however, the technologies used so far have been significantly modified and, in addition to the technologies that study the basic functions of the body, there also appear solutions allowing for mapping the areas of brain activity and determining on this basis to a limited extent both the content of the suspect's thoughts and the verification of the truthfulness of the statements made.[63]

The existing case law, including the one of constitutional courts, constitutes a good basis for the emerging technologies. In case of new measures described above and their possible implementation in the course of the criminal proceedings, there will probably be a need to reformulate the existing judgments of the courts, adapt them to new challenges, and possibly refer to new aspects of human rights protection, including the area of fair trial. Until now, the case law has focused to a large extent on a significant margin of error and not sufficient reliability of measures of

---

[62] FEDERAL CONSTITUTIONAL COURT. Judgment of 7 April 1998, 2 BvR 1827/97 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1998/04/rk19980407_2bvr182797.html r., zob. też GWIRDWOYŃ, WEIGEND, Ewa, WIDACKI, Jan, WÓJCIKIEWICZ, Józef.

German Supreme Court's alleged approval of polygraph examination in criminal proceedings, *Prokuratura i Prawo,* no. 7-8, 2009, FISCHER, Larissa BETTINA, Paul, VOIGT, TORSTEN, Voigt. Wahrheit unter dem Vergrößerungsglas. Vorstellungen von Subjekt und Technik in der Rechtsprechung zur Polygraphie, *Zeitschrift für Soziologie* v. 48, no. 5-6, p. 418-434, 2019.

[63] The existing measures allow for a much further analysis of the body's reaction, including eye-detecting technologies etc. These measures are advertised as possible to use, *i.a.* at airports in order to prevent possible criminal activities. The studies include e.g. fMRI - tracking brain activity, but also TMS, tDCS, which create the possibility of changing the activity of the brain in order to acquire particular results. BRADSHAW Robert. Deception and detection: the use of technology in assessing witness credibility, *Arbitration International*, v. 37, no. 3, p. 707-720, 2021. https://doi.org/10.1093/arbint/aiab007, FARAHANY, Nita. Incriminating Thoughts. *Stanford Law Review*, v. *64* no. 2, p. 351–408, 2012, LUBER, Bruce, FISHER, Carl, APPELBAUM, Paul, PLOESSER, Marcus, LISANBY, Sarah. Non-invasive brain stimulation in the detection of deception: Scientific challenges and ethical consequences. *Behavioral Sciences and the Law*, no. 27, p. 191-208, 2009. https://doi.org/10.1002/bsl.860

this type. In view of change in the nature and method of their operation, the question arises what statements will constitutional courts develop, if the methods used by law enforcement agencies and required expert witnesses allow for the determination of certain variables with almost absolute certainty. The question remains, how will constitutional courts define the standard of privilege against self-incrimination in this respect, and to what extent will they agree to award the suspects and defendants with the above-mentioned rights.

6. Conclusions

The progressing technological development definitely has an impact on the conduct of criminal proceedings, in particular on the scope and type of evidence invoked in individual cases. In the era of changes in procedural measures used by law enforcement agencies, it seems that the role of constitutional courts will continue to grow, affecting the protection of the rights and procedural guarantees of suspects and defendants, including ensuring the fairness of the proceedings. As it was indicated above, the new technologies that can potentially make an adverse impact on the right to a fair trial continue to appear.

As it seems, courts in their judgments concerning the use of new technologies in criminal proceedings, to a large extent rely on the already existing decisions of constitutional courts regarding fair trial and specific rights of suspects and defendants. The standards and rights affected by constitutional courts decisions are undoubtedly the right to notification, the right to information, the right to appropriate judicial review and the equality of arms. The significant impact can be also seen in the right of defense – both in terms of active participation of the suspect in the proceedings and privilege against self-incrimination. Moreover, the set of individual rights distinguished by constitutional courts on the basis of the right to privacy and the right to the protection of personal data has a fundamental impact on the fairness of the proceedings, especially considering that the existing regulations on the use of new technologies in criminal proceedings are often not yet finally clarified and they pose a risk of a threat to legal security and certainty. The principle of proportionality,

even if invoked in the context of right to privacy (for example in the context of time limits for surveillance measures taken against suspects), will have a significant role in limiting the actions of LEAs and ensuring the adequate protection of fair trial standards.

All the above mentioned factors can be observed in Polish legal system as well. The Constitutional Tribunal of Poland addressed the problems of the use of new technologies in criminal proceedings, especially the surveillance measures, mostly in the context of right to privacy. However, it does not exclude the simultaneous impact on the fair trial principles. On the contrary – the direct influence on the legislation can be noticed.

The case law of constitutional courts influences legislation in shaping the procedures for the use of digital evidence, both in terms of access to content and non-content data, and will most definitely continue to do it. It is also in some way intertwined with the judgments of European courts, in particular the CJEU. Recently, the need for mutual approximation and harmonization of procedures has also been discussed in order to ensure efficient cooperation in criminal matters and to eliminate threats to procedural rights. If this were to happen, the provisions would undoubtedly be based not only on the CJEU case law, but also on the standards developed by the constitutional courts of the Member States.

References

ACT ON THE POLICE of 6 April 1990, *Dziennik Ustaw,* item 1882

ADAM, Lisanne, BARNS, Greg. Digital strip searches in Australia: A threat to the privilege against self-incrimination, *Alternative Law Journal*, V. 45, no. 3, p. 222–227, 2020. https://doi.org/10.1177/1037969x20923073

AKTHER, Shajeda; NORDIN, Rohaida. An Analysis of Fair Trial Guarantees at Trial Stage under the ECHR, *Law Review* p. 211-234, 2015

ATTORNEY GENERAL. Motion of 12 November 2015 r., PG VIII TKw 41/14

BACHMAIER, Lorena. Exclusionary Rules of Evidence in Spain. In: THAMAN, Stephen (ed.). *Truth versus Legality in a Comparative View*, Heidelberg: Springer, p. 209–234, 2018

BACHMAIER WINTER, Lorena. Remote computer searches under Spanish Law: The proportionality principle and the protection of privacy. *Zeitschrift für die gesamte Strafrechtswissenschaft,* v. 129 no. 1, p. 205-231, 2017. https://doi.org/10.1515/zstw-2017-0008

BANASZAK, Bogusław. *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa: C.H.Beck, p. 212, 2012

BARAK, Aharon. *Proportionality. Constitutional Rights and Their Limitations*, Cambridge: Cambridge University Press, p. 472, 2006

BARKHUYSEN, Tom, EMMERIK, VAN, Michiel, JANSEN, Oswald, FEDOROVA, Masha. Right to a Fair Trial. In: DIJK, VAN, Pieter, HOOF, Van, Fried RIJN, VAN, Arjen, ZWAAK, Leo. *Theory and practice of the European Convention on Human Rights*, Cambridge: Intesentia, p. 637, 2018

BULGARIAN SUPREME ADMINISTRATIVE COURT. Decision No 13627, 11 December 2008

BRADSHAW Robert. Deception and detection: the use of technology in assessing witness credibility, *Arbitration International*, v. 37, no. 3, p. 707-720, 2021. https://doi.org/10.1093/arbint/aiab007

BREMS, Eva. Conflicting human rights: an exploration in the context of the right to a fair trial in the European Convention for the protection of human rights and fundamental freedoms. *Human Rights Quarterly*, v. 27, n. 1, p. 294-326, 2005, https://doi.org/10.1353/hrq.2005.0003

CARNES, Brittany A. Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones, *Loyola Law Review,* v. 66, n.1, p. 183-210, 2020

CHOPRA, Pran. The Constitution and Supreme Court. *Economic and Political Weekly*, *v. 39* no. 30, p. 3355–3359, 2004. http://www.jstor.org/stable/4415313

CHOUDHRY, Sujit (ed.). *The Migration of Constitutional Ideals*, Cambridge: Cambridge University Press, 2006

CONSTITUTION OF THE REPUBLIC OF POLAND of 2nd April 1997, published in *Dziennik Ustaw* No. 78, item 483

CONSTITUTIONAL COURT OF ROMANIA. Decision No 1258 of 8 October 2009

CONSTITUTIONAL COURT OF SPAIN. Judgment 253/2006 of 11 September 2006

CONSTITUTIONAL COURT OF SPAIN. Decision STC 114/184

CONSTITUTIONAL COURT OF THE CZECH REPUBLIC. Decision of 22 March 2011, Pl. ÚS 24/10

CONSTITUTIONAL COURT OF THE CZECH REPUBLIC. Decision of 22 December 2011, Pl. ÚS 24/11

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 11 February 1992 r., K 14/91

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 26 January 1993, U 10/92

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 17 October 1995, K 10/95

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 25 November 2003, K 37/02

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of May, 17 2004, SK 32/03

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of December, 12 2005 r., K 32/04

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 9 July 2009, SK 48/05

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 25 July 2013, P 56/11

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of April 30, 2014, K 23/11

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 5 June 2014 r., K 35/11

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 14 July 2015, SK 26/14

CONSTITUTIONAL TRIBUNAL OF POLAND. Judgment of 4 November 2015, K 1/14

CONSTITUTIONAL TRIBUNAL OF POLAND. Decision of June, 30 2021 r., K32/05

COURT OF JUSTICE OF THE EUROPEAN UNION, Judgment of 8 April 2014, joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of 21 December 2016, joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, EU:C:2016:970

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of October, 6 2020, *La Quadrature du Net and Others v Premier ministre and Other*s, joined cases C-511/18, C-512/18 i C-520/18, EU:C:2020:791

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment of 6 October 2020, Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, EU:C:2020:790

COURT OF JUSTICE OF THE EUROPEAN UNION. Judgment (Grand Chamber), 2 March 2021, C-746/18, *Criminal proceedings against H. K.,* EU:C:2021:152

CZERNIAK, Dominika. Collection of location data in criminal proceedings – European (the EU and Strasbourg) standards. *Revista Brasileira de Direito Processual Penal*, v. 7, n. 1, p. 123-160, 2021. https://doi.org/10.22197/rbdpp.v7i1.503

DEENER, David. Judicial Review in Modern Constitutional Systems. *The American Political Science Review*, v. 46 no, 4, 1079–1099, 1952. https://doi.org/10.2307/1952114

DE VRIES, Katja, BELLANOVA Rocco, DE HERT Paul, GUTWIRTH Serge. The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?). In: GUTWIRTH Serge, POULLET Yves, DE HERT Paul, LEENES Ronald (eds) Computers, Privacy and Data Protection: an Element of Choice, p. 3-23, 2011, https://doi.org/10.1007/978-94-007-0641-5_1

DIRECTIVE 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, Available at: http://data.europa.eu/eli/dir/2006/24/oj

DISTRICT COURT OF APPEAL OF FLORIDA, *State v. Stahl,* 206 So. 3d 124, 136-37 (Fla. Dist. Ct. App. 2016)

DIXON, Rosalind. Updating Constitutional Rules. *The Supreme Court Review*, no. 1, p. 319–346, 2009. https://doi.org/10.1086/653651

EUROJUST. Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report, 2017. Available at: <https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf> >. Accessed March 15, 2022

EUROPEAN CONVENTION OF HUMAN RIGHTS, adopted in Rome on 4th November 1950. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf >

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 8 February 1996, *John Murray v. the United Kingdom* (app. no. 18731/91)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 29 June 2006, Weber and Saravia v. Germany, (app. no. 54934/00)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 29 June 2007, O'Halloran and Francis v. the United Kingdom, (app. nos. 15809/02 and 25624/02)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 4 December 2008, S. and Marper v. the United Kingdom (app. nos. 30562/04 and 30566/04)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 17 December 2009, B.B. v. France (app. no. 5335/06),

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 17 December 2009, Gardel v. France and M.B. v. France (app. no. 22115/06)

EUROPEAN COURT OF HUMAN RIGHTS Judgment of 2 Sptember 2010, Uzun v. Germany (app. no. 35623/05)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 21 June 2011, Shimovolos v. Russia (app. no. 30194/09)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 3 July 2012, Robathin v. Austria (app. no. 30457/06)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 18 April 2013, M.K. v. France (app. no. 19522/09)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 18 September 2014, Brunet v. France (app. no. 21010/10)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 12 January 2016, Szabó and Vissy v. Hungary (app. no. 37138/14)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 30 May 2017, Trabajo Rueda v. Spain (app. no. 32600/12)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 22 June 2017, Aycaguer v. France, (app. no. 8806/12)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 13 February 2020, Gaughran v. the United Kingdom (app. no. 45245/15)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 25 May 2021, Centrum För Rättvisa v. Sweden (app. no. 35252/08)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 16 November 2021, Vasil Vasiliev v. Bulgaria, (app. no. 7610/15)

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 14 October 2021, Lysusk v. Ukraine, (app. no. 72531/1)

EUROPEAN COURT OF HUMAN RIGHTS. Press Unit, Factsheet – new technologies, 2021. Available at: <https://www.echr.coe.int/documents/fs_new_technologies_eng.pdf> AccessedJanuary 9, 2022

EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. Opinion EESC 2018/02737, OJ C 367, 10.10.2018, p. 88–92. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11314_2021_INIT&from=EN.

FARAHANY, Nita. Incriminating Thoughts. *Stanford Law Review*, v. *64* no. 2, p. 351–408, 2012

FEDERAL CONSTITUTIONAL COURT. Judgment of 7 April 1998, 2 BvR 1827/97 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1998/04/rk19980407_2bvr182797.html

FEDERAL CONSTITUTIONAL COURT. Judgment of the First Senate of 27 February 2008, 1 BvR 370/07, 1 BvR 595/07

FEDERAL CONSTITUTIONAL COURT. Judgment of the First Senate of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09

FEDERAL CONSTITUTIONAL COURT. Press release no 11/2010 of 2 March 2010

FEDERAL COURT OF AUSTRALIA, Luppino v Fisher (No 2) [2019] FCA 1100

FISCHER, Larissa BETTINA, Paul, VOIGT, TORSTEN, Voigt. Wahrheit unter dem Vergrößerungsglas. Vorstellungen von Subjekt und Technik in der Rechtsprechung zur Polygraphie, *Zeitschrift für Soziologie* v. 48, no. 5-6, p. 418 – 434, 2019

FUNDACJA PANOPTYKON. Telefoniczna Kopalnia Informacji. Przewodnik, p. 20. Available at: https://panoptykon.org/biblio/telefoniczna–kopalnia–informacji–przewodnik. Accessed: March 15, 2022

GARLICKI, Lech; WOJTYCZEK, Krzysztof. Komentarz do art. 31 Konstytucji. In: GARLICKI, Lech; ZUBIK, Marek (ed.). *Konstytucja Rzeczypospolitej Polskiej*. Komentarz, t. II, Warsaw: Wolters Kluwer Polska, p. 69, 2016

GERSTEIN, Robert. Privacy and self-incrimination. In SCHOEMAN, Ferdinand David (ed.), *Philosophical Dimensions of Privacy:* An Anthology, Cambridge: Cambridge University Press, p. 245-264, 1984. doi:10.1017/CBO9780511625138.010,

GOLDMAN, Kara. Biometric passwords and the privilege against self-incrimination. *Cardozo Arts & Entertainment Law Journal*, v. 33, no. 1, p. 211-236, 2015

GWIRDWOYŃ, WEIGEND, Ewa, WIDACKI, Jan, WÓJCIKIEWICZ, Józef.

German Supreme Court's alleged approval of polygraph examination in criminal proceedings, *Prokuratura i Prawo,* n. 7-8, 2009

HARRIS, David. The right to a fair trial in criminal proceedings as a human right, *International & Comparative Law Quarterly*, v. 16 n. 2, p. 352-378, 1967, https://doi.org/10.1093/iclqaj/16.2.352

HERRERA, Adam. Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination, *UCLA Law Review,* v. 66 n. 3, p. .778-817, 2019

INDIANA COURT OF APPEALS. *Seo v. State, 109* N.E.3d 418, 425-31 (Ind. Ct. App. 2018) *2018* WL 6565988 (Ind. Dec. 6, 2018)

JACKSON, Vicki. *Constitutional Engagement in a Transnational Era*, Oxford: Oxford University Press, p. 60, 2010

JUSZCZAK, Adam, SASON, Elisa. Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning? *EUCRIM* v. 4, p. 238 – 266, 2021, https://doi.org/10.30709/eucrim-2021-020

KUMM, Mattias. Constitutional Rights as Principles, *International Journal of Constitutional Law* v. 2, p. 595, 2004, https://doi.org/10.1093/icon/2.3.574

LACH, Arkadiusz. *Rzetelne postępowanie dowodowe w sprawach karnych w świetle orzecznictwa strasburskiego*, Warszawa: Wolters Kluwer Polska, p. 112-158, 2019

LOFTUS, Bethan. Normalizing covert surveillance: the subterranean world of policing, *The British Journal of Sociology,* p. 2070-2091, https://doi.org/10.1111/1468-4446.12651

LUBER, Bruce, FISHER, Carl, APPELBAUM, Paul, PLOESSER, Marcus, LISANBY, Sarah. Non-invasive brain stimulation in the detection of deception: Scientific challenges and ethical consequences. *Behavioral Sciences and the Law*, no. 27, p. 191-208, 2009. https://doi.org/10.1002/bsl.860

MAHONEY, Paul. Right to a fair trial in criminal matters under Article 6 ECHR. *Judicial Studies Institute Journal*, v. 4, n. 2, p. 107-129, 2004

MASSACHUSETTS SUPREME JUDICIAL COURT. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614-15 (Mass. 2014)

MARAS, Marie-Helen. From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?. In GOOLD, Benjamin J., NEYLAND, Daniel (eds). *New Directions in Surveillance and Privacy*, Willan, 2009. https://doi.org/10.4324/9781843927266

MITROU, Lilian. The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive. In HAGGERTY, Kevin, SAMATAS, Minas Samatas (eds). *Surveillance and Democracy*, New York: Routledge, 2010

OFFICE OF ELECTRONIC COMMUNICATION. *Report of June 2021*. Available at: <https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/391/10/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2020_roku_.pdf>. Access on March 15, 2022

OLBER, Paweł. Remote Search of IT System in Polish Legislation and Its Importance in Fight Against Cybercrime, *Internal Security,* v. 11, n. 2, p. 141-140. http://dx.doi.org/10.5604/01.3001.0013.8288

OMBUDSMAN OF POLAND. Motion of 4 December 2015 r., II.511.84.2015.KSz

PEW RESEARCH CENTER FO INTERNET AND TECHNOLOGY. *Mobile Fact Sheet, Pew Research Center for Internet and Technology of February 5, 2018*. Available at: <https://www.pewinternet.org/fact-sheet/mobile>. Access on March 15, 2022QUEENSLAND COURT OF APPEAL. Wassmuth v Commissioner of Police [2018] QCA 290

REGULATION (EU – proposal) of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD)

RANGAVIZ, David. Compelled decryption & state constitutional protection against self-incrimination. *American Criminal Law Review*, v. 57, no. 1, p. 157-206, 2020

RECHTBANK NOORD-HOLLAND [District Court of North-Holland, the Netherlands]. Judgment of 25 January 2019, NJFS 15/168454-18

REDMAYNE, Mike. Rethinking the Privilege Against Self-Incrimination, *Oxford Journal of Legal Studies*, v. 27, no. 2, p. 209–232, 2007 https://doi.org/10.1093/ojls/gql001

ROCHON, Mark, SCHMITT, Andy, HERBERT, Ian. Is It Time to Revisit the Corporate Privilege Against Compelled Self-Incrimination? *The Champion,* p. 50 – 59, 2019

ROJSZCZAK, Marcin. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. *European Constitutional Law Review*, p. 607-635, 2021. https://doi.org/10.1017/S157401962100035

ROJSZCZAK, Marcin. *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warsaw: Wolters Kluwer Polska, 2019

SKRĘTOWICZ, Edward. Z problematyki rzetelnego procesu karnego. In: SKORUPKA, Jerzy (ed.). *Rzetelny proces karny. Księga jubileuszowa Profesor Zofi i Świdy*, Warsaw: Wolters Kluwer Polska, p. 23, 2009,

STOYKOVA, Radina, Digital evidence: Unaddressed threats to fairness and the presumption of innocence, *Computer Law & Security Review*, v. 42, 2021. https://doi.org/10.1016/j.clsr.2021.105575

ŚLEDZIŃSKA SIMON, Anna. *Analiza proporcjonalności ograniczeń konstytucyjnych praw i wolności. Teoria i praktyka*, p. 24, 2019. https://doi.org/10.34616/23.19.020

TAYLOR, Mark. The EU Data Retention Directive *Computer Law & Security Review,* v. 22 p. 309-312, 2006. https://doi.org./10.1016/j.clsr.2006.05.005

TULEJA, Piotr. Komentarz do art. 31 Konstytucji. In: TULEJA, Piotr (ed.). *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warsaw: Wolters Kluwer Polska, p. 114.119, 2019.

UNITED STATES COURT OF APPEAL FOR THE ARMED FORCES, *United States v. Mitchell H, 76* M.J. 413,424-25 & n.5 (C.A.A.F. 2017)

UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT, *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011,* 670 F.3d 1335, 1349 (11th Cir. 2012)

UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT, *United States v. Apple MacPro Computer,* 851 F.3d 238, 248 & n.7 (3d Cir. 2017 138 S. Ct. 1988 (2018)

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLORADO, *United States v. Fricosu,* 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012)

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN. *United States v. Kirschner,* 823 F. Supp. 2d 665 (E.D. Mich. 2010)

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, *United States v. Spencer,* No. *17-cr-00259-CRB-1,* 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018)

VAINIO, Niklas, MIETTINEN, Samuli. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States, *International Journal of Law and Information Technology*, v. 23, no. 3, p. 290–309, 2015. https://doi.org/10.1093/ijlit/eav010

VERBRUGGEN, Frank; CONINGS, Charlotte. After zigzagging between extremes, finally common sense? Will Belgium return to reasonable rules on illegally obtained evidence? *Revista Brasileira de Direito Processual Pena*l, v. 7, n. 1, p. 273-310, 2021. https://doi.org/10.22197/rbdpp.v7i1.500

VICTORIAN COURT OF APPEAL, McElroy v The Queen; Wallace v The Queen [2018] VSCA 126, 55 VR 450

VITKAUSAS, Dovydas; DIKOV, Grigoriy. *Protecting the right to a fair trial under the European Convention on Human Rights. Council of Europe*. Available at: <https://edoc.coe.int/en/module/ec_addformat/download?cle=c82b013313066e0702d-58dc70db033ca&k=2fc0fa200f64659df501f62a8386baad>. Accessed March 23, 2022

WILIŃSKI, Paweł. *Proces karny w świetle Konstytucji*, Warsaw: Wolters Kluwer Polska, p. 174-177, 2011

WILIŃSKI, Paweł. *Zasada prawa do obrony w polskim procesie karnym*, Warsaw: Wolters Kluwer Polska, p. 354-359, 2006

WÓJTOWICZ, Krzysztof. Zasada proporcjonalności jako wyznacznik konstytucyjności norm. In: ZUBIK, Marek (ed.). *Księga XX-lecia orzecznictwa Trybunału Konstytucyjnego*, Warsaw: Biuro Trybunału Konstytucyjnego, p. 265–278, 2006

ZUBIK, Marek; PODKOWIK, Jan; RYBSKI, Robert. *European Constitutional Courts towards Data Retention Laws*, Cham: Springer, 2021, https://doi.org/10.1007/978-3-030-57189-4

Authorship information

Michalina Marcia. PhD student at the Chair of Constitutional Law (Faculty of Law, Administration and Economics, University of Wroclaw), Research Assistant at the Digital Justice Center. michalina.marcia@uwr.edu.pl

Additional information and author's declarations
(scientific integrity)

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 with 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; she also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Submission: 14/01/2022
- Desk review and plagiarism check: 30/01/2022
- Review 1: 19/02/2022
- Review 2: 28/02/2022
- Review 3: 28/02/2022
- Review 4: 06/03/2022
- Review 5: 09/03/2022
- Preliminary editorial decision: 09/03/2022
- Correction round return: 25/03/2022
- Final editorial decision: 02/04/2022

Editorial team
- Editor-in-chief: 1 (VGV)
- Associated-editor: 1 (MKJ)
- Reviewers: 5

HOW TO CITE (ABNT Brazil):

MARCIA, Michalina. The role of constitutional courts in taming adverse impact of new technologies in the criminal proceedings. *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 1, p. 153-188, jan./abr. 2022. https://doi.org/10.22197/rbdpp.v8i1.678