Studia Iuridica 86
ISSN 0137-4346; e-ISSN 2544-3135

DOI: https://doi.org/10.31338/2544-3135.si.2020-86.2

Jan Czarnocki
KU Leuven Centre for IT & IP Law, Belgium[1]
ORCID:0000-0002-3570-2198

ELECTRONIC COMMUNICATION CONFIDENTIALITY IN ePRIVACY REGULATION: HOW TO PROTECT PRIVACY AND PERSONAL AUTONOMY WITHOUT HAMPERING AI SOLUTIONS DEVELOPMENT[2]

Abstract

This article aims to analyse Articles 5 and 6 of the draft ePrivacy Regulation put forward by the European Commission, as key rules regulating the processing of electronic communication data and metadata. The confidentiality of electronic communication is an important aspect of privacy and personal autonomy protection. Still, disproportionate regulation may hurt economic growth, particularly with regard to artificial intelligence (AI) solutions development. The article begins by briefly describing a socio-economic context in which the future regulation of electronic communication confidentiality will function, then analyses the implications of proposed norms for the protection of privacy and personal autonomy, and their potential implications for economic development, for AI solutions in particular. The article analyses which of the proposed versions of Articles 5 and 6 meet the middle ground and ensure protection of privacy and personal autonomy without at the same time hampering economic development

[1] KU Leuven Centre for IT & IP Law – IMEC, Sint-Michielsstraat 6 box 3443, 3000 Leuven, Belgium.

[2] This article is part of the PriMa ITN project and received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 860315.

and AI innovation. After analysing the proposed normative content of all three versions of the ePrivacy Regulation draft, some afterthoughts are shared about them and their potential impact. The goal is to find the proper balance between privacy protection as an ultimate priority and maintaining economic development and innovation as something that cannot be ignored and is a priority in its own right, to an extent where it does not harm the essential content of the fundamental right to privacy and personal autonomy.

KEYWORDS

privacy, personal autonomy, GDPR, artificial intelligence, eprivacy regulation, data

SŁOWA KLUCZOWE

prywatność, autonomia osobista, GDPR, sztuczna inteligencja, rozporządzenie e-privacy, dane

1. INTRODUCTION[3]

This article aims to analyse Articles 5 and 6 of the draft ePrivacy Regulation put forward by the European Commission, as key rules regulating the processing of electronic communication data and metadata. Although the European Union (EU) Member States withheld their acceptance of the European Commission (Commission)'s draft and the new draft is still to be introduced[4], the old draft proposed by the Commission, along with the amendments made by the European Parliament (Parliament) and the European Council (Council), gives us a valuable and relevant view and context of how the issue of electronic communication confidentiality will be further regulated. While the work on the ePrivacy Regulation continues and its end is not yet in sight, the positions taken by all the involved institutions give us an insight into how each of them envisions further data regulation. The confidentiality of electronic communication is an important aspect of privacy and personal autonomy protection. At the same time, disproportionate

[3] I would like to thank Aleksander Milanowski for his editorial advice and help on this article.

[4] A. Samuelson, *Commission to present revamped ePrivacy proposal*, EURACTIV.com 2019, https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/ (visited 28 December 2020).

regulation may hurt economic growth, particularly with regard to artificial intelligence (AI) solutions development.

Privacy of communication is a value enshrined in and protected by Article 7 of the Charter on Fundamental Rights of the European Union (Charter)[5], related directly to the protection of privacy and correspondence guaranteed in Article 8 of the European Convention on Human Rights (ECHR)[6]. Articles 5 and 6 of the draft ePrivacy Regulation, which are *lex specialis* to the General Data Protection Regulation (GDPR)[7], are crucial general rules for the privacy and data protection. They would have a serious impact on economic growth, AI development in particular. While the importance of confidentiality of electronic communication for the protection of the fundamental rights seems to be clear[8], the impact of its normative enactment on innovation and development of the digital economy is not clear enough so far. This article aims to point to the possible impact of these legal norms and reflect on which proposed versions of Articles 5 and 6 of the ePrivacy Regulation, establishing the rule of the confidentiality of electronic communication, regulate it in a way that protects fundamental rights enshrined in the Charter and the ECHR, but also give regard to the overall economic interests of the broader society and does not hamper the future development of AI solutions.

The article begins by briefly describing a socio-economic context in which the future regulation of electronic communications confidentiality will function. It then analyses how the proposals of the legacy draft of the ePrivacy Regulation, as well as the Parliament's and Council's amendments, impact the Commission's initial version. Further, the article analyses the proposed norms' implications for the protection of privacy and personal autonomy, and their potential implications for economic development, AI solutions in particular. The article analyses which of the proposed versions meet the middle ground and ensure protection of privacy and personal autonomy without at the same time hampering economic development and AI innovation. After analysing the proposed normative content of all the three versions of the ePrivacy Regulation draft, some afterthoughts about them and their potential impact are shared. The goal is to find the proper balance between privacy protection as an ultimate priority and maintaining economic development and innovation as something that cannot be ignored and is a priority in its own right, to an extent where it does not harm the essential content of the fundamental right to privacy and personal autonomy. It is possible to design sound legal norms that will, at the same time, sufficiently protect the privacy

[5] Article 7, Charter of the Fundamental Rights of the European Union.

[6] Article 8, European Convention on Human Rights.

[7] Article 5, Proposal for a Regulation on Privacy and Electronic Communications, European Commission 2017, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation/ (visited 28 December 2020).

[8] D. J. Solove, *Understanding Privacy*, Harvard University Press 2008, pp. 78–101.

and personal autonomy, and allow economic development with AI solutions in particular.

2. ELECTRONIC COMMUNICATION CONFIDENTIALITY: SECURING BOTH PERSONAL AUTONOMY AND ECONOMIC DEVELOPMENT

Data is the fuel of digital economy and a critical resource for its growth[9]. The knowledge-based, post-industrial society[10] relies on it increasingly in the development of services and industries[11]. Data is also a *sine qua non* resource for development of AI solutions like autonomous cars, search engines, virtual assistants, and predictive algorithms[12]. Algorithm-based AI analytical tools are trained based on data input, through which they can learn and enhance themselves[13]. Without falling into popular, exaggerated hype over AI solutions[14], we can say that, as a matter of fact, they are important technologies which may boost productivity and enable exploring new uncharted territories of sustainable economic growth[15]. Gaining supremacy in AI solutions may be vital not only for maintaining the economic competitiveness of the European Union but also for its defence and security[16]. Still, numerous social externalities may arise if unrestricted data gathering is permitted. Loss of privacy, both at an individual and group level, is a fact inherently connected with the *laissez-faire* style approach to data gathering, processing, and analysis[17]. Unrestricted data gathering and accumulation

[9] J. Rifkin, *The Zero Marginal Cost Society: The Internet of Things, The Collaborative Commons, and The Eclipse of Capitalism*, New York 2014, pp. 69–135; L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford 2016, pp. 25–58.

[10] D. Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, New York 1998.

[11] K. Schwab, *The Fourth Industrial Revolution*, World Economic Forum 2016, p. 31.

[12] S. Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*, Penguin Publishing Group 2019, p. 34; A. Agrawal, J. Gans, A. Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence*, Harvard Business Press 2018, p. 23.

[13] *Ibidem*.

[14] L. Floridi, *Charting Our AI Future*, Project Syndicate 2017, https://www.project-syndicate.org/commentary/human-implications-of-artificial-intelligence-by-luciano-floridi-2017-01 (visited 28 December 2020).

[15] A. Agrawal, J. Gans, A. Goldfarb, *Prediction Machines*..., p. 43.

[16] Ch. Brose, *The Kill Chain: Defending America in The Future of High-Tech Warfare*, Hachette Books 2020, p. 55.

[17] B. van der Sloot, *Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR*, (in:) L. Taylor, L. Floridi, B. van der Sloot (eds.), *Group Privacy*, Springer 2017, Philosophical Studies Series, Vol. 126.

also creates huge asymmetries of power and influence between social strata, tearing apart trust and the social fabric[18]. The complexity of the situation needs to be acknowledged to enable a pragmatic and workable approach considering the consequences of regulation of data processing, in this case the processing of electronic communication data. There is a need to evaluate the appropriateness of potential regulations with view to practical effects that they may have on overall individual and social welfare.

Privacy and personal autonomy are the key values at stake in the context of a platform-based digital economy[19]. Autonomy can be conceptualized as a bundle of rights, protected *inter alia* by Articles 8, 9, and 10 of the ECHR[20]. Personal autonomy is defined here as the inviolable part of the most inner self, separated from what is outside the individual, and which ought to be protected from harmful intrusions. This sphere of internal thoughts, feelings, and affections, towards which we can retreat and reflect on the environment and reality around us, is what constitutes our self, and based on which, as agents capable of self-reflection, we differentiate ourselves as individuals against our surroundings and our systemic and environmental conditions[21]. Contemporary data gathering, processing, and analysis technologies create a situation in which it is possible to collect and infer knowledge about individuals and the whole society with precision and in amounts not comprehensible and possible before[22]. This possibility creates numerous opportunities to benefit overall human welfare[23], but at the same time, it creates considerable risks for privacy and personal autonomy. These risks are created by asymmetries of knowledge between users and data holders like platforms and data monopolies[24]. Digital platforms can nudge and manipulate people into certain choices through predictive algorithms and an optimized online and offline choice architecture, enabled by our communication devices and development of the Internet of Everything[25]. Therefore, it is urgent to mitigate those risks and

[18] S. Zuboff, *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*, Profile Books 2019, pp. 27–62.

[19] *Ibidem*; J. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford 2019, p. 75.

[20] Articles 8, 9, 10, European Convention on Human Rights.

[21] M. Archer, *Being Human: The Problem Of Agency*, Cambridge 2001, pp. 22–40; H. G. Frankfurt, *Freedom of the Will and the Concept of a Person*, "The Journal of Philosophy" 1971, Vol. 68, No. 1, pp. 5–14; G. Dworkin, *The Theory and Practice of Autonomy*, Cambridge 1988, pp. 10–32.

[22] L. Floridi, *The Fourth Revolution*…, pp. 25–58.

[23] S. Russell, *Human Compatible*..., p. 42; A. Agrawal, J. Gans, A. Goldfarb, *Prediction Machines*..., p. 28.

[24] A. Ezrachi, M. E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, Massachusetts 2016, pp. 3–22; N. Srnicek, *Platform Capitalism (Theory Redux)*, Polity 2016, p. 36.

[25] D. Kahneman, *Thinking, Fast and Slow*, Farrar, Straus and Giroux 2011, pp. 39–89; R. H. Thaler, C. R. Sunstein *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Penguin Books 2009, pp. 11–35; S. Zuboff, *The Age of Surveillance Capitalism*..., pp. 123–150.

introduce smart regulations enabling economic growth and AI solutions development while effectively protecting privacy and personal autonomy, both at the group and individual levels. A future ePrivacy Regulation will be a part of this effort.

So far, data as content of the electronic communication has served as an important economic resource and input for training and development of numerous AI solutions like search engines and smart e-mail replies. It gives AI solutions a massive amount of knowledge about human behavior, its patterns, and correlations. As the semantic capabilities of AI solutions so far are negligible, if any at all[26], it is the syntactic content of electronic communication data from which knowledge about the users is inferred, which is valuable and makes it possible to make inferences and predictions about users' behavior. By connecting numerous patterns and correlations, users' psychological and behavioral profiles can be created[27]. With knowledge gained through ads and choice architecture and design, deployed AI algorithms can market and offer products and services, nudging and steering users into certain sets of behaviors optimal for their owners. This is the core of the business model of numerous companies, especially digital platforms[28]. The reader may reflect here on how often it has happened to them that they mentioned in correspondence or voice messages on a given platform something about a particular product or their consumption needs, and after that, the advertisement of that kind was displayed on the same platform, or even in a browser or on another platform. Therefore, the general rule prohibiting the processing of electronic communication data must change, both for privacy protection and for the availability of data for training the algorithms, as less accurate data will be possible to be gathered. However, not all data processing may be a privacy breach, therefore there is a need for a regulation both protecting our privacy and at the same time allowing the developing of better AI solutions, not necessarily focused only on the sales maximization, but which can be beneficial to overall social welfare[29].

[26] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson 2020, pp. 13–40.

[27] M. Hildebrandt, S. Gutwirth, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer 2008, pp. 1–10.

[28] M. Hildebrandt, *Smart Technologies and End(s) of Law*, Elgar 2015, pp. 38–75.

[29] "We could imagine the possibility of restricted access for purposes that do neither aim at interfering with individuals' privacy rights, nor have the effect of such interference. An example is access with the rationale of delivering better services, such as machine learning applications or personal assistance (like automated translations or voice to text applications). Of course, it should be ensured that individuals' rights are effectively protected, including effective remedies". Centre For Information Policy Leadership, The ePrivacy Regulation and the EU Charter of Fundamental Rights, 9 November 2018, p. 11.

3. REGULATING THE CONFIDENTIALITY OF ELECTRONIC COMMUNICATION

The proposed ePrivacy Regulation is to be related to the GDPR on a *lex specialis derogat legi generali* basis[30]. The analysis here is confined to the norms of the draft ePrivacy Regulation considered to be making the most significant changes in the legal landscape of data and privacy protection and setting up the general abstract rules of electronic data confidentiality. These rules will determine interpretation and application of other, more detailed rules of future ePrivacy Regulation and the current GDPR. Articles 5 and 6 of the draft ePrivacy Regulation are posed to be the key norms in the legacy ePrivacy regulation draft, by setting up general and abstract rules of electronic communication data confidentiality and defining exemptions from them. Although the wording of the proposed Articles 5 and 6 may change in the future draft, it is assumed that the versions put forward and amended in the legacy draft cannot substantively differ much from the future proposals, as the need for the confidentiality of electronic communication puts certain logical and linguistic constraints on the possible formulation of these norms. These logical and linguistic constraints make the analysis and *de lege ferenda* postulates in this paper relevant for the purpose of further reflections on the future ePrivacy Regulation.

Article 5 of the ePrivacy Regulation, proposed by the Commission, sets up a general principle prohibiting access to electronic communication data by anyone other than the parties communicating with each other[31]. The amended version of Article 5, proposed by the Parliament, makes the provision much more precise, enumerating possible ways of interference and adding that any interference, except if done by the end-users, is prohibited[32]. The Parliament also amended Article 5 to apply to data stored in the terminal equipment, which is important because by virtue of this amendment the electronic communication can be duly

[30] Article 5, Proposal for a Regulation on Privacy…

[31] "Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation". Article 5, Proposal for a Regulation on Privacy…

[32] "Electronic communications shall be confidential. Any interference, with electronic communications, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or any processing of electronic communications, by persons other than the end-users, shall be prohibited". Article 5, Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), European Parliament 2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html/ (visited 28 December 2020).

protected in its full scope[33]. While the Commission's proposal stipulates a clear principle of confidentiality of electronic communication data, it still does allow certain exceptions, stipulated further in the Regulation. The Parliament's proposal seems much stricter, with the changed wording describing the confidentiality principle as applicable to electronic communications in general[34]. The word "data" is omitted, making the potential scope of application much broader and eliminating possible disputes over lack of clarity as to what may be counted as data, and what may not. In the Parliament's amended version it is also automatically clear that metadata are confidential, whereas the Commission's version stipulated separate legal norms for the regulation of metadata processing, precluding the assumption that its version also covers metadata. Although in its normative value the principle of confidentiality, proposed by the Commission, has the same content, the wording used by the Parliament's amendment sounds much stricter, canceling the sentence about possible exemptions to be stipulated further, although particular exemptions are still further listed in the Parliament's version. This stricter wording, without mentioning potential exemptions in one article, does not change much *de iure*, but it does *de facto,* because of its strict framing. It may change the actual and overall way of the law's application, potentially influencing a stricter interpretation on a case-by-case basis. This remark supports the pragmatic view of legal practice, according to which looking at potential consequences of the application of the legal norm helps design them with these consequences in mind[35].

While Article 5 of the draft ePrivacy Regulation states the general key rule, Article 6 lists the exemptions and conditions to be fulfilled to make the electronic communication data processing exonerated, permitted, or lawful, depending on the version of the draft and amendments added by either the Parliament or the Council. Article 6 is the crucial one for preservation of privacy, as it will ultimately regulate what can and what cannot be done with electronic communication data. It is also in Article 6 that we see the widest divergences between normative positions taken by the Commission, the Parliament, and the Council, accordingly. Each of these positions would probably mean something different for privacy and personal autonomy protection on the one hand, and the economic development, especially in the field of AI solutions development, on the other hand.

The Commission's proposed legacy draft Article 6.1 enumerates the allowed exceptions to Article 5. Electronic communication data may be processed when

> (a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or

[33] Article 5, Report on the proposal for a regulation…

[34] *Ibidem*.

[35] O. W. Holmes, *The Path of Law*, "Harvard Law Review" 1897, 10-457, pp. 1–20.

errors in the transmission of electronic communications, for the duration necessary for that purpose[36].

In its reformulation of Article 6, the Parliament proposes that it is permitted to process electronic communication data only if "it is technically necessary to achieve the transmission of the communication, for the duration necessary for that purpose"[37]. Article 6.1b, as amended by the Parliament, puts stricter conditions on the processing, limiting it only to the situations, when it is

technically necessary to maintain or restore the availability, integrity, confidentiality, and security of the respective electronic communications network or services, or to detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose[38].

Parliament's version, however, broadens the subjective scope of the Article, permitting access for the parties acting on behalf of the provider or the end-user[39]. Therefore, the Parliament's proposal puts stricter conditions on the processing, detailing that the confidentiality principle does not apply if the knowledge about content of communication is needed for the technical provision of the service. At the same time, it broadens the scope of the principle, to allow third parties, acting on behalf of the provider, as sub-contractors for example, to maintain security of the connection. The Parliament's version, in this case, seems to do justice to the needs of the market, where sometimes it is necessary to provide access to third-party contractors to secure, maintain or fix the technical and security issues in the network.

The Council amendments substantially reformulate Parliament's proposal, listing a broad catalog of situations in which the processing of electronic communication data is permitted. According to the Council, processing of electronic communication should be permitted if

(a) it is necessary to achieve the transmission of the electronic communication; or (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or security risks and/or attacks in the transmission of electronic communications; (c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment (…)[40].

[36] Article 6, Proposal for a Regulation on Privacy…

[37] Article 6, Report on the proposal for a regulation…

[38] *Ibidem*.

[39] *Ibidem*.

[40] Article 6, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 6543/20, The Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-6543-2020-INIT/en/pdf/ (visited 28 December 2020).

The formulation of the Article 6, in the Council's version, by giving a catalog of exemptions and because of using different wording, is less restrictive than the previous versions of the Commission and the Parliament. The Council's proposal states that processing of data is permitted if it is necessary to achieve the connection, without differentiating between whether it is a technical or any other necessity. It also makes precise that it is also legal to interfere in communications' content if there is a security risk for the relevant network and interference is needed for its detection. Also in its added Article 6.2 and Article 6.3, the Council postulates that

> Electronic communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6bc and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous. (…) A third party acting on behalf of a provider of electronic communications network or services may be permitted to process electronic communications data in accordance with Articles 6 to 6bc provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met[41].

This means that, in principle, regardless of the previously mentioned exemptions, all lawful processing ought to be done firstly through the processing of anonymized data. Not anonymized data can only be used when it is not otherwise possible to achieve the purpose of the processing. Council's amendment also leaves the door for third party access, which the Parliament's amendments also permitted, but it does so with the clarification that these potential third-parties also ought to be subject to the legal requirements stipulated for the data processor, as understood and regulated in the GDPR.

Another exemption to the general prohibiting rule from Article 5 is the possible consent of the user. The EU lawmakers presented three visions of the extent to which consent should waive the general prohibiting rule to process electronic communication data laid down in Article 5. Regardless of numerous legal scholars' opinions that the consent is not a sufficient condition to secure privacy[42], it is still the standard applied in the GDPR and one that will probably be applied in the ePrivacy Regulation. The failure of consent to protect privacy to the extent needed, is assigned *inter alia* to information and power asymmetries between the provider of the service or product and the user. The elusiveness of knowledge on what the user is giving consent, as well as the use of tracking walls by providers

[41] Article 6.3, Proposal for a Regulation of the European Parliament (…) 6543/20…

[42] M. Nouwens, I. Liccardi, M. Veale, D. Karger, L. Kagal, *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Association for Computing Machinery, New York, pp. 1–13.

are other factors limiting the relevance and effectiveness of consent as a tool to protect privacy[43]. In the Commission's proposal Article 6.3 states that

> Providers of the electronic communications services may process electronic communications content only: (a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or (b) if all end--users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority[44].

The idea of consent proposed by the Commission is one of general protection and confidentiality of electronic communication, regardless of the consent given for processing. Consent can be given for the processing of data for a particular purpose, or for the sake of upholding and providing the electronic communication service itself. In these cases, the prohibition is waived. The data can also be processed if the user gave consent to the processing for the specific purpose of providing a particular service, but only if the given service cannot be provided with the processing of anonymized data. This means that even if the user consents to the processing of data for a specified purpose, should it be feasible to provide a given service without the processing of not anonymized data, the processing is required to be anonymous. Furthermore, the Commission's version of the draft obliges the processing party to consult the relevant supervisory authority before processing, to comply with the requirements stipulated in Article 36 of the GDPR[45]. Parliament's version specifies that the service to be provided, where the electronic communication data is about to be processed, is the service that was explicitly requested by the user[46]. It also states that the consent of the user is only applicable to their own data. Hence, for the processing of electronic communication data, the provider needs consent of both parties, that are taking part in communication. The Parliament's amendment also creates an exemption in Article 6.3a, adding that

[43] F. J. Zuiderveen Borgesius, S. Kruikemeier, S. C. Boerman, N. Helberger, *Tracking Walls: Take-it-or-Leave-it hoices, the GDPR, and the ePrivacy Regulation*, 3(3) Eur. Data Prot. L. Rev. 353 (2017).

[44] Article 6.3, Proposal for a Regulation on Privacy…

[45] Article 36, Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union.

[46] Article 6.3a, Report on the proposal for a regulation…

> 3a. The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users[47].

Whereas the Commission's wording was strict and plain in this regard, Parliament's version creates a gate for provision of particular services, where only one side of the communication consented. In principle, processing is possible even without the consent of other end-users involved, as long as it does not infringe on their fundamental rights.

The Council's amendments permit to process the data under consent, even if it is not the case that both parties gave it, as long as the processing does not affect the fundamental rights of the part withholding consent, but only to the extent that the processing of data is connected to a specified purpose for which it was gathered[48]. The Council amendment also does away with the obligation to first carry out processing of anonymized data, if it is necessary for the service provision, as the Commission's and Parliament's versions were proposing. If consent and other legal requirements are met, the Council's version permits non-anonymized data procession. Its version also puts an obligation on the provider to carry out risk assessment and consult the relevant supervisory authority before processing, according to Article 36 of the GDPR. In general, the Council's amendments broaden the scope of possible consent, stating that consent is valid for the processing the data related to specifically indicated service and for these specific purposes that the data subject consented to. This is a much less restrictive approach, where both Commission's and Parliament's proposals stipulated a narrow catalog of situations where processing is permitted, surrounding it with precise conditions to be fulfilled anyway, even should consent be given. With the Council's amendments, the requirements are less strict, with only the purpose-based limitation of gathering as a guiding principle.

Metadata is a by-product created by the processing of data. Meta-data is no less important because it can carry the information about matters like with whom the electronic communication took place and when, where it happened, and what the size of the file being sent is. Collection and analysis of metadata and metadata patterns greatly enhance the possibility to create psychological and behavioral profiles of users[49], therefore regulation of its processing is no less important than the regulation of data processing itself. According to Article 6.2, as proposed by the Commission's draft, the providers of electronic communications may process metadata if

---

[47] *Ibidem*.

[48] Article 6a, Proposal for a Regulation of the European Parliament (…) 6543/20…

[49] M. Hildebrandt, S. Gutwirth, *Profiling the European Citizen*..., pp. 1–10.

> (a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212011 for the duration necessary for that purpose; or (b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or (c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous[50].

This proposal gives much broader permitted use of metadata than the content of the communication itself. The meta-data can be processed if it is necessary for the service provision, its quality, and its security. It is also permitted to process it if the end-user consents. Still, metadata can only be processed only if the service demanded cannot be provided by the processing of anonymized data or metadata. Parliament's wording of the same provisions keeps it more precise that data can be processed, but only if it is strictly and technically necessary, leaving the same other conditions for lawful processing[51]. It also lifts the Commission's requirement that the processing of metadata has to be tried out first on the anonymized data and metadata[52]. However, the Parliament's version requires the conducting of risk assessment and notification of relevant supervisory authorities before processing of the metadata, as required by the GDPR[53].

The Council amendments do substantially change the conditions and the scope proposed by other lawmakers. Its proposal adds the legitimate interest of network or service provider, as a basis for permitted processing of metadata, as long as this interest is not overridden by the fundamental rights of the end-user[54]. Further, the Council specifies that legitimate interest of the provider is overridden where the metadata collected is being used to determine the nature and characteristics of the end-user, or it is used for profiling the end-user[55]. The interest of the provider is also overridden if the metadata consists of special categories of personal data, as outlined in Article 9(1) of the GDPR[56]. The Council's version also loosens the strictness and the technical necessity condition of the version proposed by the Parliament, stating only that the processing is permitted if it is necessary for the provision of the service that the end-user chose through the contract[57]. The novelty brought by the Council amendments concerning the processing of metadata is the

[50] Article 6.2, Proposal for a Regulation on Privacy…
[51] Article 6, Report on the proposal for a regulation…
[52] Article 6.2c, *ibidem*.
[53] Article 35, 36, Regulation (EU) 2016/679…
[54] Article 6, Proposal for a Regulation of the European Parliament (…) 6543/20…
[55] *Ibidem*.
[56] Article 9(1), Regulation (EU) 2016/679…
[57] Article 6, Proposal for a Regulation of the European Parliament (…) 6543/20…

prohibition of disclosing metadata by the provider to third parties, unless they are anonymized and due regard has been given to the risk assessment and lawful processing conditions as stated in the Articles 35 and 36 of the GDPR[58]. Still, the Council's proposals create a duty to inform the end-user of such disclosure and give the user the right to object to this kind of processing of their metadata. There should be proper technical conditions set up, so that the objection may be given easily and effectively. The provider should further make sure that these processed metadata are duly pseudonymized and encrypted[59].

By analysing Articles 5 and 6 it can be seen that Parliament's version generally supplements and complements the Commission's version. The amendments proposed by the Parliament to Articles 5 and 6 bring more detail and more potential interpretative strictness, but they do not change the substance and scope of the rights and obligations. Whereas some minor differences may still be seen between Commission's and Parliament's versions, the Council's amendments are reframing the scope and the content of rights and obligations deriving from Articles 5 and 6 of the draft. Commission's and even more so Parliament's drafts create a strong rule of electronic data confidentiality, allowing a limited scope of exemptions and limiting even the effectiveness of what can be done with the electronic communication data even with the user's consent in place. Conversely, the Council puts forward the legitimate interest basis as a possibility for processing, opening up a vast scope of opportunities for processing. Still, the Council's amendments seem to more strongly align the rule of confidentiality to the other rules in the GDPR, the *lex generalis* to the future ePrivacy Regulation. Therefore, even if the conditions for processing set up by the Council are less strict, its framing of Articles 5 and 6 promises a more coherent application of these provisions through their strict alignment with the GDPR, also creating an explicit obligation for the parties willing to process data to comply with the requirements of risk assessment and supervisory authority notification as stipulated in Articles 35 and 36 of the GDPR. Whereas Commission and Parliament's drafts limit the possibility to process the electronic communication data and metadata to only what is strictly necessary, the Council's version allows interference of third party interest, as long as it does not override the essence of fundamental rights, in this case, rights derived from Article 7 and the Charter of Fundamental Rights[60]. Allowing the processing of anonymized and pseudonymized metadata for scientific and statistical purposes was also included in the Council's proposal[61]. According to the reports issued by the Council, the negotiations failed because the Member

[58] *Ibidem*.

[59] *Ibidem*.

[60] Article 7, Charter on the Fundamental Rights of the European Union.

[61] Article 6bf, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communica-

States could not agree on the content and the scope of the exemptions from Article 5 to be included in Article 6. Progress reports are showing that the issue of adding legitimate interest as a basis for data processing was the main cause of the failure of the negotiations.

4. ARTICLES 5 AND 6 POTENTIAL IMPACT ON PERSONAL AUTONOMY PROTECTION AND AI INNOVATION

General prohibition of interception and processing of electronic communication data, including data stored on the terminal equipment, will be an important and necessary milestone for protection of privacy, and in consequence protection of personal autonomy. The confidentiality of correspondence is connected to privacy security, especially in the context of the digital economy, where our communication content can be automatically intercepted and processed on a broad scale. This general prohibitive rule is also important because it is in the content of our communication that we tend to reveal to the outside world what we feel and think about, also by that sharing the knowledge about ourselves. So far, the European Union's legal framework has not protected the content of electronic communication sufficiently enough and it has been possible to process the content of our electronic communication and infer knowledge about us based on what we disclose in our electronic communications. While normally it seems to us that this content is secure and protected from an outside look, it turns out that in the contemporary economic framework it is constantly subject to automated surveillance and analysis by service providers and other third parties. From this perspective, the Commission and Parliament's amended versions seem to set up the strictest regimes for the confidentiality of electronic communication, with a limited scope of lawful exemptions.

At the same time, it is necessary to answer the question whether the proposed prohibition in Article 5 and the exceptions to it in Article 6 are not too restrictive and whether they will not hamper the European Union's digital sector development and competitiveness, AI solutions in particular. The ePrivacy regulation draft, primarily through norms that are analysed in this paper, may create an overall strict regime for electronic communication data processing and an overall impression of hostility toward any kind of data processing to an entity eager to do so. These new rules, along with the GDPR, may create what can be called a chilling effect on data-dependent AI solutions innovation. These are and clearly still will be the arguments for relaxing the electronic communications confiden-

tions). Presidency discussion paper, 9243/20, The Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-9243-2020-INIT/en/pdf/ (visited 28 December 2020).

tiality regime, for example along the lines proposed in the amendments of the Council. Its version does protect the electronic communication data, but broadens the exemptions and aligns them more with data processing conditions from the GDPR. Still, the principal question is whether any electronic communication data ought to be permitted to be processed, regardless of whether there exists the processor or third party's legitimate interest. It is difficult, however, to imagine what this legitimate interest could be unless it is an economic one. That would clearly not qualify as more important than the protection of privacy and correspondence. Still, the argument of overall economic growth and welfare, that the growth and gains in productivity may become more and more dependent on AI solutions, may be raised by opponents of such strict regulation. This big picture argument may be legitimate, to some extent, as in the long run the privacy and personal autonomy protection may turn out to be a luxury that the European Union will not be able to afford further if in the future it will lose its economic and competitive edge. It may be simply that the competition void in certain sectors, left by the EU, will be filled by the competitors that do not care about privacy and personal autonomy protection as much as we do, as it is actually happening[62]. Therefore, proper regulation, which protects the privacy and personal autonomy in a smart way, at the same time allowing AI innovation, is important.

Regardless, when focusing on AI solutions it is necessary to understand that their effectiveness is dependent on the purpose for which they have been developed and dependent on data, that they have been trained on[63]. Therefore, limiting access of algorithms to the data from the electronic communications may indeed hamper AI solutions development, but perhaps only those which purpose is to analyse and infer predictions about personal behavior of consumers, helping to manipulate them into buying certain products and services. It is hardly imaginable that the prohibitions and exemptions from Articles 5 and 6 will hamper development of, for example, industrially applicable AI solutions, as data from the electronic communications might be irrelevant for the training of such AI. From this perspective it may well be that it is not important that algorithms passively process electronic communication data, if their purpose is not to profile and target us, actively infringing on our privacy and personal autonomy. If we do not want the AI solutions that will be efficient and effective in targeting individuals based on their behavioral patterns, then maybe the smarter way is to prohibit the collection of data for this purpose and for training algorithms for this purpose, but allow the collection of these data, if they are duly pseudonymized and anonymized, for the purpose of training algorithms for other purposes that may be beneficial to the society and economic growth. From this perspective, the Council's proposal seems to be the most rational one, as it upholds the general rule of confidentiality

[62] S. Zuboff, *The Age of Surveillance Capitalism*..., pp. 27–62.
[63] S. Russell, P. Norvig, *Artificial Intelligence*..., pp. 13–40.

of electronic communication data, while still allowing the broad scope of exemptions, with a legitimate purpose, backed up by the risk assessment and notification of supervisory authorities, as legal enablers of electronic communication data gathering. These solutions may be seen as a balanced middle ground, because no supervisory authority, seeing a filled in risk assessment, would allow for the training of algorithms based on electronic communication data, aimed at targeting users with its producer's services and products. At the same time, it is highly likely that the same authority will accept the legitimate interests of the processor and third party should it be a scientific purpose or other purpose, as long as it is not one infringing on privacy and personal autonomy in a malicious way. That is why it is even more regrettable that the Council's proposals appeared only after the Commission's draft was scraped by it and the new process of reworking of ePrivacy Regulation was announced because the negotiations failed[64].

5. CONCLUSION

The general rule of electronic communication confidentiality is a sine qua non condition for privacy and personal autonomy protection. Still, simply allowing everything or prohibiting everything is not the way. The Council's proposal of Article 5 and 6 seem to be the closest to the smart regulation that will at the same time protect electronic communication data, so the privacy and personal autonomy, but as well will not excessively hamper economic growth, particularly AI solutions development that might be beneficial for overall economic welfare, while especially targeting development with the purpose of building behavioral profiles of the users, predicting their behavior and targeting them with products and services based on obtained information. It is to be seen however what ideas the Commission will come up with in the new draft of the ePrivacy Regulation. A more nuanced and smart approach, distinguishing between desirable and undesirable use of data, as well as between potentially beneficial and harmful AI solutions is needed, with protection of privacy and personal autonomy remaining the priority.

REFERENCES

Agrawal A., Gans J., Goldfarb A., *Prediction Machines: The Simple Economics of Artificial Intelligence*, Harvard Business Press 2018

[64] A. Samuelson, *Commission…*

Archer M., *Being Human: The Problem of Agency*, Cambridge 2001
Bell D., *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, New York 1998
Brose Ch., *The Kill Chain: Defending America in the Future of High-Tech Warfare*, Hachette Books 2020
Centre For Information Policy Leadership, *The ePrivacy Regulation and the EU Charter of Fundamental Rights*, 9 November 2018
Charter of the Fundamental Rights of the European Union
Cohen J., *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford 2019
Dworkin G., *The Theory and Practice of Autonomy*, Cambridge 1988
Ezrachi A., Stucke M. E., *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, Massachusetts 2016
Floridi L., *Charting Our AI Future*, Project Syndicate 2017, https://www.project-syndicate.org/commentary/human-implications-of-artificial-intelligence-by-luciano-floridi-2017-01 (visited 28 December 2020)
Floridi L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford 2016
Frankfurt H. G., *Freedom of the Will and the Concept of a Person*, "The Journal of Philosophy" 1971, Vol. 68, No. 1
Hildebrandt M., *Smart Technologies and End(s) of Law*, Elgar 2015
Hildebrandt M., Gutwirth S. (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer 2008
Holmes O. W., *The Path of Law*, "Harvard Law Review" 1987, 10-457
Kahneman D., *Thinking, Fast and Slow*, Farrar, Straus and Giroux 2011
Nouwens M., Liccardi I., Veale M., Karger D., Kagal L., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Association for Computing Machinery, New York
Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Presidency discussion paper, 9243/20, The Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-9243-2020-INIT/en/pdf/ (visited 28 December 2020)
Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 6543/20, The Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-6543-2020-INIT/en/pdf/ (visited 28 December 2020)
Proposal for a Regulation on Privacy and Electronic Communications, European Commission 2017, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation/ (visited 28 December 2020)
Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union

Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), European Parliament 2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html/ (visited 28 December 2020)

Rifkin J., *The Zero Marginal Cost Society: The Internet of Things, The Collaborative Commons, and The Eclipse of Capitalism*, New York 2014

Russell S., *Human Compatible: Artificial Intelligence and the Problem of Control*, Penguin Publishing Group 2019

Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson 2020

Samuelson A., *Commission to present revamped ePrivacy proposal*, EURACTIV.com, https://www.euractiv.com/section/data-protection/news/commission-to-present-revamped-eprivacy-proposal/ (visited 28 December 2020)

Schwab K., *The Fourth Industrial Revolution*, World Economic Forum, 2016

Sloot B. van der, *Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR*, (in:) L. Taylor, L. Floridi, B. van der Sloot (eds.), *Group Privacy*, Springer 2017, Philosophical Studies Series, Vol. 126

Solove D. J., *Understanding Privacy*, Harvard University Press, 2008

Srnicek N., *Platform Capitalism (Theory Redux)*, Polity 2016

Thaler R. H., Sunstein C. R., *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Penguin Books 2009

Zuboff S., *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*, Profile Books 2019

Zuiderveen Borgesius F. J., Kruikemeier S., Boerman S. C., Helberger N., *Tracking Walls: Take-it-or-Leave-it Choices, the GDPR, and the ePrivacy Regulation*, 3(3) Eur. Data Prot. L. Rev. 353 (2017)