THE ROLE OF PRIVACY IN THE ESTABLISHMENT OF THE RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

Andrej Krištofík*

Abstract: *Despite the rise in processes that are being automated in our daily life not much attention has been directed at the regulation of automation as such, that is not tied expressly to the technology that is being used for the automation. This holds true for automated decision-making, which can in its public form have a great impact on the individual's life. As such, automated decision-making has only been regulated as a part of privacy-oriented legal instruments, which naturally begs the questions, whether the right to not be subject to automated decision-making is in fact a privacy related right. The article attempts to answer this question by identifying the place of the right to not be subject to automated decision-making within one of the privacy types, identified in extensive typology of Koops et al. It further posits several other legal values, that are different from privacy, that could warrant the placement of this right within the existing legal instruments.*

Keywords: *Privacy, automated decision making, autonomy, artificial intelligence, data protection*

I. INTRODUCTION

The focal point at the center of law is, at least within the framework of European "kantian" legal culture, the human being.[1] This anthropocentric principle informs, as a basic starting point, all aspects of it. The subject of law is the human being, and to this end, law shapes all its values, rules and purposes. The centrality of human emerges especially in the context of distributive rights. While non-distributive rights also acknowledge the significance of the human, distributive rights assume a more pronounced role in enhancing human autonomy and related aspects. This is achieved, in part, through the ability to exclude others, effectively elevating the individual's central role and autonomy within the legal framework. The centrality of the human being thus finds particular prominence within the realm of different distributive rights, emphasizing their crucial role in shaping the legal landscape.

Such centrality is also referred to by Warren and Brandeis in their description of the development of law, or in their description of how law has gradually expanded (and is expanding) from the basic protection of "vi et armis" to other, more advanced institutions of law, that are ultimately designed to meet constantly evolving, social needs.[2] Based on their description of this development of law, Warren and Brandeis arrive at the first conceptualization of the right to privacy – following the, now somewhat amusing, fact of the proliferation of photography and the journalistic business at that time. The increasing complexity of life and the progress of civilization requires the creation of a larger space for man in which he "would be left to himself", outside the prying eyes of the public sphere.[3] This new

* Mgr. Andrej Krištofík, Ph.D. student at the Institute of Law and Technology, Masaryk University, Brno, Czech Republic. ORCID: 0000-0001-8150-0362. This article was written as a part of the Masaryk University research project "Právo a Technologie XII" number MUNI/A/1529/2023 supported by the special-purpose support for specific university research provided by the Ministry of Education of the Czech Republic in 2024.

[1] POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012. pp. 300–301.

[2] WARREN, D. S., BRANDEIS, L. D. The right to privacy. *Harvard Law Review*. 1890, Vol. 4, No. 5, pp. 193–195.

[3] Ibid., p. 196.

civilizational need, the right to privacy, is becoming more widespread, with the advance of technological developments that even Warren and Brandeis could not have foreseen, especially in light of the amount of data that is being captured, pertaining to individuals, whether or not it is their will.[4] Despite this widespread need for it, the concept of privacy, and the right to it, is difficult to conceptualize and therefore difficult to grasp.[5] Often, however, privacy is understood as being contextual, or being understood as a contextual integrity.[6] This brings us back to the centrality of the human being, since contextual integrity as a concept of privacy, builds on the fact that no human being is an "island entire of itself",[7] which is to say that it is essential for the fulfillment of the essence of human as a social being, that one be able to share information with other human beings – at one's own discretion.[8] It is thus a difficult balancing exercise, from which the rather alibist way out is through the establishment of as extensive autonomous space as permissible for the person, as it regards his or hers choice pertaining to the discretion of informational disclosure.[9]

These interests should be balanced by the set up of an appropriate legal framework as well, in particular within the context of the European Union, which actively strives to uphold these core values.[10] Within this framework, then, the European legislator seeks to limit intrusions into the sphere of privacy, among other things also by regulating the possibilities of automated decision-making. Within these regulations, it is then not uncommon to encounter an explicit establishment of the right to not be subject to automated decision-making.[11] Such provisions occur repeatedly in legislation aimed at protecting privacy or personal data. That raises a question of whether automated decision-making

[4] HENSCHKE, A. *Ethics in an Age of Surveillance*. Cambridge: Cambridge University Press, 2017, p. 4.

[5] KOOPS, B. J. et al. *A Typology of Privacy. PennLaw: Legal Scholarship repository*. Tilburg: Tilburg University, 2017. p. 487.

[6] NISSENBAUM, H. *Privacy in context: Policy, Technology, and the Integrity of Social Life*. Standford: Standford University Press, 2010, p. 304.

[7] DONNE, J. *Devotions Upon Emergent Occasions by John Donne*. In: *Project Guttenberg* [online]. [2023-06-11]. Available at: <www.gutenberg.org/files/23772/23772-h/23772-h.htm>.

[8] Privacy must therefore be an (autonomous) human choice. Too restrictive a view of privacy is seen, besides being contrary to the nature of the human person, as too paternalistic, and some authors point out that some people may simply want to share their data, for example even with multinational corporations, and preventing them from doing so is an unacceptable interference with their autonomy. Cf SOLOVE, D. J. *The digital person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004, pp. 91 and following.

[9] FEINBERG, J. Personal Sovereignty and Its Boundaries. In: Joel Feinberg (ed.). *The Moral Limits of the Criminal Law Volume 3: Harm to Self*. Oxford: Oxford University Press, 1989, pp. 52–97.

[10] BARKAN, M. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*. 2019, No. 27, pp. 91–93.

[11] In addition to the Article 22 of EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1 (hereinafter "GDPR"), which will be the subject of further discussion, cf e.g. Article 9 of the Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108, or "comparatively" cf AI Bill of Rights and the setting of automated decision-making as a mandated opt-out system. OSTP WH. *Blueprint for an AI Bill of Rights* In: *The White House* [online]. 2023 [2023-06-11]. Available at: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>, p. 46, or similarly Article 11 in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 2 119/89/01 (hereinafter "police directive").

can be considered an invasion of privacy or if it serves as a safeguard for other human-centric values, such as personality rights or human autonomy. Should it be deemed a protection of privacy, then it should be essential to establish, what kind of privacy we are dealing with.[12] Engaging with this typological question ought to help us firstly establish whether it truly aims at the protection of privacy, which then in turn ought to help us properly strike a balance between the imperatives of privacy (should it be relevant) and other legally relevant values in the realm of automated decision-making and law itself.

Concept of privacy presents a considerable challenge in terms of its conceptualization, prompting significant scholarly efforts to address this issue. In their work "A Typology of Privacy", Koops et al. have made a notable contribution to this effort. The authors offer a comprehensive typology of privacy, drawing upon an analysis of constitutional orders from various countries and an examination of scholarly literature. Their typology, formulated from the perspective of fundamental rights, provides a valuable framework for our exploration. In the following work we will make use of this framework of conceptualization of privacy and attempt to firstly classify the (prohibition of) automated decision making within one of those types, thus concluding whether the goal of placing this prohibition into legal instruments primarily concerned with the protection of privacy is justified.[13] After the introduction of the problem it will be required, for proper classification, to establish the concept of automated decision making, which will form part of the section 2.2. Lastly the article will deal with the question whether such placement of this regulation within the privacy protection oriented tools was justified by other privacy-adjacent values, such as autonomy or human agency, will be analyzed subsequently in the last part of the text.

II. THE RIGHT TO BE FREE FROM AUTOMATED DECISION-MAKING

A certain discrepancy in the nature of the right not to be subject to automated decision-making can also be observed in the provisions of the two, currently central, legal instruments. Those being, Article 22 of the GDPR, which frames this right as one of the rights of the data subject, whereas Article 11 of the Police Directive, containing a similar provision, is situated within the section outlining the fundamental principles of data protection.[14]

[12] KOOPS, B. J. et al. *A Typology of Privacy.*

[13] There is obviously the pragmatist approach to this question to consider, firstly these instruments as being exclusively oriented towards data protection, without the extensive goal of privacy protection and in this vein the regulation of automated decision making could thus be seen as regulated thereof solely due to its operation on and with personal data. Such view is however too restrictive not only for the goals and purposes of these legal tools that are better understood as privacy oriented, but also for the scope of automated decision making that does not have to necessarily be individual. For the impact and role of data processing in automated decision making for example cf VEDDER, A. *Why Data Protection And Transparency Are Not Enough When Facing Social Problems Of Machine Learning In A Big Data Context. Being Profiled.* Amsterdam: Amsterdam University Press, 2018. In: *chooser.crossref.org* [online]. 27. 12. 2018 [2024-04-18]. Available at: <http://dx.doi.org/10.2307/j.ctvhrd092.10>. Or alternatively cf Ploug who, whilst discussing the impact on privacy, still chooses as the regulatory point the use of (public) data. PLOUG, T. The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling. *Philosophy & Technology.* Vol. 36, No. 1. In: *Springer Link* [online]. [2024-04-18]. Available at: <https://dx.doi.org/10.1007/s13347-023-00616-9>.

[14] It is also possible to perceive a difference in their "force", since the Police Directive states an explicit prohibition, whereas GDPR, as much as it is often referred to as setting a ban on automated decision making, viewed prag-

The Guidelines for Automated Decision Making issued by the Working Party 29, asserts that the GDPR establishes a general prohibition on automated decision making, and then subsequently identifies exceptions to that prohibition.[15] The perception of the need for protection against automated decision-making by the European legislator is thus apparently relatively strong.[16] Exploring the safeguards mandated by the GDPR when automated decision-making is deemed permissible can provide insights into the values intended to be safeguarded by these provisions and the underlying establishment of such a right in the first place. In cases where automated decision-making is permissible by law, "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."[17] In the other cases, i.e. in situations where automated decision-making is permissible based on the consent of the affected party, or necessary in the context of performance of a contract, it is required to ensure "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".[18]

At least in the latter case, the focus primarily revolves around the possibilities of ensuring substantive human intervention, if not substantive[19] input, into the decision-making process.[20] For this guarantee, it is then questionable to what extent it really constitutes a legal guarantee, and to what extent it constitutes a guarantee which primary purpose is to protect some other legally relevant value, and to what extent it is intended to mitigate the potential problem of distrust in (new) technologies. Brkan, for instance, interprets this right as an integral part of the right not to be the subject to automated decision-making, as it establishes the possibility of human intervention that takes the subject out of the reach of *solely* automated decision-making. The author, however, sees this as more of a procedural guarantee of a "second instance", which must logically be mediated by a human being in most cases.[21] Since this safeguard represents only a subsequent pos-

matically it more or less just sets up the necessary conditions that are to be met for legitimately carried out automated decision making, even with full legal effects on its subject. At a minimum, then, this creates a difference in the active and passive nature of this protection as it pertains to the necessary will of the subject. On this, cf for example BRKAN, M. *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*. pp. 97–8.

[15] Working Party 29, *Papers of the Article 29 Working Party*: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* 2018, p. 19.

[16] At least in a footnote, it is worth to draw attention to the fact that this protection was originally directed towards, or evolved from, protection against profiling. Cf BRKAN, M. *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*. p. 98.

[17] GDPR, Art. 22(2)(b).

[18] Ibid., Art. 22(3).

[19] For the issue of "substantivity" of the intervention see the problem of mere "rubber stamping" for example in BRENNAN-MARQUEZ, K. et al. Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision Making. *Berkeley Technology Law Journal*. 2019, Vol. 34, No. 3, p. 745.

[20] Brkan argues, for example, that the real purpose of these safeguards is to protect against discrimination and bias in automated decision-making. While not incorrect, in the author's view this view covers only part of the purpose of these safeguards. Cf BRKAN, M. *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*.

[21] There are three possible scenarios for an appellate proceeding in automated decision making. First, the "easiest" scenario is such a case in which there are new facts that came to light and are still eligible to be considered (and this in itself creates the reason for appeal). We label this as the "easiest" scenario since it only requires a second run of the very same decision-making algorithm or system, with new information, in order to satisfy the requirement of the second instance. The other two, more "complicated" cases are perhaps those envisioned by the GDPRs' requirement of human intervention, those being such cases that require assessment by a "second pair

sibility of escaping the solely automated decision-making means and not an a priori possibility, this right cannot be considered an independent right that directly shields individuals from automated decision-making.[22]

The remaining conditions of protecting the rights and freedoms (and legitimate interest), are in principle very indirect, if not alibist, approaches, as Koops makes a similar point when he speaks of the concept of privacy as undefinable in itself, or as of one that can only be captured by the conjunction of a whole host of other surrounding concepts.[23] The question that has already been raised above and which has so far failed to move closer to being answered, is whether any of these associated concepts can be attributed to a value safeguarded by the right not to be the subject of automated decision-making. Addressing this question becomes particularly imperative in light of the perceived "hollowing out" of this right, which some authors trace to the extensive exceptions to this right as well as to its problematic relationship with the right to a fair trial or the provisions outlined in the Article 48 of the European Charter of Fundamental Human Rights.[24,25]

II.1 Protection of Privacy

Koops et al. have introduced a conceptual framework of the fundamental types of privacy, drawing on their comprehensive survey on the perception of the concept of privacy across various constitutional orders or constitutions and across a body of scholarly works on the topic. These distinct types epitomize the ideal[26] type that embody the core values inherent in this particular legal discourse. The representation of these types is mapped onto a two-dimensional plane – with a horizontal axis defining privacy zones, and a vertical axis reflecting the continuum of negativity and positivity of protection, referred to as the "freedom" axis,[27] capturing the polarity between negative and positive dimensions of privacy safeguards.

---

of eyes". This could potentially lead us to utilizing a different decision-making algorithm for the second instance, that would however implicitly mean that this second algorithm is in some way better, more just or more precise, naturally posing the question of why not use this algorithm in the first instance. This leads us to the third scenario, which is the "the only logical solution" of having the second instance assessed by a human. To bring this to conclusion we also must ask the very same question of why not put the human in the first instance since it, again, ought to be better. Without going into the "linguistics" of better/more suitable/different, the main reason of why this argument does not hold as much power as it did in the second scenario is the fact that while we can swap an algorithm for a better one essentially in a 1:1 manner, we can't do the same for human and algorithm. Therefore, creating this double instance scenario allows us to utilize the benefits of algorithmic decision making such as speed and certainty, whilst retaining a reasonable second instance, and satisfying amongst else, the right to a fair trial. Further discussion of this issue is however out of the scope of this particular paper.

[22] BRKAN, M. *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*.

[23] KOOPS, B. J. et al. *A Typology of Privacy*. p. 488.

[24] For this discussion cf e.g. BRKAN, M. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond.

[25] Alternatively, this linkage is interesting in the context of China and its cybersecurity laws, which, while introducing strong data protection, provide virtually no privacy protection. Cf PARASOL, M. Data Protection but Not Data Privacy: Data Protection Shall Not Hinder AI. In: Max Parasol *AI development and the 'fuzzy logic' of Chinese cyber security and Data Laws*. Cambridge: Cambridge University Press, 2023. p. 154.

[26] KOOPS, B. J. et al. *A Typology of Privacy*. p. 495.

[27] Ibid., p. 566.

In addition, this typology has a further diagonal division into the spectrum of *control* and *access*. This spectrum expresses the two basic defining elements of privacy, or its purpose, namely (limiting) control over access to certain information in the first place, and subsequent control over the information once it has been disclosed.

On the horizontal axis, Koops et al. present the core areas of privacy arising from the content analysis of constitutional orders and their approaches to privacy, or to be more precise, based in which areas are they trying to establish a certain privacy zone in persons' life. These include personal, intimate, semi-private and public zones. These areas are meant to represent the increasing degree of an individual's involvement in the public sphere of life. However, such a division of privacy is not sufficient, or rather, for the purposes of legal values analysis, it is necessary to conceptualize the various components of privacy further, along the axis of freedom, that is, "freedom from" and "freedom to". While such a binary division is relatively commonplace in conceptualization of privacy, it is by far not the only one, and as Koops points out in the article, it is to some extent surpassed by the privacy triad proposed by MacCallum (freedom *of something – from something – to(wards) something*).[28] However, Koops et al. attempt to overcome this lack of binary division of freedom exclusively into negative and positive by constructing positivity and negativity axis as a spectrum.

The addition of this axis results in the formulation of the comprehensive 8+1 core types of privacy, collectively encompassing all conceivable approaches and conceptualizations of privacy across diverse constitutional frameworks. If the right not to be the subject to automated decision-making is a right primarily oriented towards preservation of privacy, it should be possible to subsume it under one of the types thus identified. Given that the "+1", the ninth concept of privacy, is informational privacy, which, according to Koops' typology, overlaps with all the remaining concepts of privacy,[29] informational privacy will be discussed last.

Among the types that are meant to emphasize negative aspects of freedom -that is, freedom from - Koops identifies *bodily*, *spatial*, *communicational*, and *proprietary* privacy. In all of these areas, there should be a broader emphasis on freedom *from* some interference by another party. The very designation of the right to *not be* a subject (of automated decision-making) implies freedom *from*, that is, freedom from being such a subject (of automated decision making). However, categorizing this right under the second axis of the typology or subsuming it within any of the four types centered on the negative definition of privacy presents challenges. Bodily privacy refers to the physical aspects of a person's existence, their corporeality and its protection[30] and as such, this type of privacy can be more or less directly excluded from further consideration as the relevant privacy type for the concept of privacy pertaining to automated decision making.[31] Similarly, spatial privacy concerns the protection of physical space inhabited by individuals, also making it an

[28] Ibid., p. 556.
[29] Ibid., p. 484.
[30] Ibid., p. 498.
[31] Even though there can be an impact on corporeality of the subject as well as the physical aspects of their being, those impacts are the result of said decision, not the (automatisation of) the process itself, as will be the case with some other aspects.

unlikely candidate for association with privacy typology of automated decision-making. Moving further along the axis of individuals ingress into the public sphere, we move away from types of privacy relating mainly to physical realities of one's life. The first type of privacy on this end of spectrum is privacy protecting communication, i.e., the fact that an individual's (private) communication will not be eavesdropped on or interfered with, without the knowledge of those communicating. Clarke identifies a core (legal) value for this type of privacy to be "self-respect" and "self-realization".[32] If we are to be concerned solely with the *process* of automating the decision-making per se (and protection from it) this type does not seem to be appropriate. In contrast, however, the greater possibilities for surveillance (of private communications) in the so-called "algorithmic society" can be seen as certainly expanding the possible impact on this aspect of privacy.[33] However, this relates more to changes in rules and processes in wiretapping and other invasive information-gathering methods related to private communications of the individual, which could result in more invasive automated decision-making, rather than to decision-making as such, without any changes to these procedures. Thus, for the protection against automated decision-making per se, communication privacy is not the relevant type. The final type of privacy on the negative end of the spectrum is proprietary privacy. This type of privacy refers to property rights, or the ability to use property as a means of protecting one's own privacy.[34] Again, this is clearly a type unsuitable for automated decision making. While it may ultimately affect an individual's ability to use property and related rights in this way, that i.e. in order to protect his or hers privacy, this is not an impact directly resulting from the automation of decision-making but an impact stemming rather from the (modified) possible consequences of such decisions, and therefore this type is not relevant for placement of automated decision-making itself.

At this point, we should move on from the conception of the right to *not be* the subject of automated decision-making as negatively conceptualized right to privacy. However, aligning this right with the positive conceptualisations of the right to privacy is not necessarily contradictory (to its designation as a right *not to be)*. Indeed, it can be tentatively assumed that by creating protection from some interference, for example, by creating protection *from* automated decision-making, the maintenance of the positive space of the right - that is, the right *to* something – is facilitated, in a similar triadic way, to what MacCallum suggest as being the case for the "freedom" axis of the right to privacy.[35]

On the positive end of the vertical axis spectrum, Koops et al. situate the *intellectual, decisional, associational*, and *behavioral* types of privacy. The essential immateriality of their object(s)[36] is to some extent derived precisely from the shift on the vertical axis to the sphere of positive freedom, i.e., freedom *to* something. This part of the spectrum posits

[32] CLARKE, R. What's Privacy. In: *Australian Law Reform Commission* [online]. 28. 7. 2006 [2023-06-11]. Available at: <http://www.rogerclarke.com/DV/Privacy.html>.
[33] SIMONCINI, A., LONGO, E. Fundamental Rights and the Rule of Law in the Algorithmic Society. In: Hans-Wolfgang Micklitz et al. (eds.). *Constitutional Challenges in the Algorithmic Society.* Cambridge: Cambridge University Press, 2021, p. 28.
[34] KOOPS, B. J. et al. *A Typology of Privacy.* p. 567.
[35] Ibid., p. 556.
[36] Ibid., p. 555.

the concept for self-development as its core goal,[37] and delineates the individual's space within it. Moore, in his definition of privacy and its end goals, points out that it is privacy (or the individual's ability to limit access by others to himself) that creates the space for personal growth, and at the same time, it preserves a level of personal autonomy (concerning the course of ones life) for the individual.[38]

In the light of defining privacy as a possibility of exclusion, it is then interesting to note that the two effects mentioned above, personal growth and autonomy, are not necessarily complementary; rather, they appear to exist at opposite ends of the spectrum. An appropriately conceived notion of privacy must not only protect privacy, but also enable an individual to freely communicate information selected by him or her and simulatenously receive such information from and about other members of society, precisely with the aim of fulfilling the purpose of self-development as well as due to the inherent informational essence of life and the essence of information itself.[39]

The first of the identified types, intellectual privacy, has emerged relatively recently in the literature compared to other privacy types and was often initially described as an amalgamation of other conceptions of privacy.[40] At its core, this type of privacy also presents a similar tension between negativity and positivity as discussed previously in relation to the negativity of prohibition of automated decision-making and its subsumption under the positive aspects of freedom. Intellectual privacy is often seen as being in a conflict with, or in opposition to, the rights related to freedom of expression[41] (and access to information, which this right equally represents).[42] Richards points out, however, that it is precisely the negativity of intellectual privacy protection that helps to facilitate the space needed for freedom of expression.[43] Fundamentally, this type of privacy aims to safeguard the integrity of an individual's intellectual pursuits, which need not be confined exclusively to the realm of their mind. Moreover, it extends protection against interference with an individual's discussions, planning, and development of ideas with others of his or hers choosing (hence the original conceptualization of this type of privacy as a kind of hybrid between other types and concepts, namely, between informational and associational types of privacy).

The different types of privacy located on the lower part of the vertical axis of Koops' typology exhibit significantly higher interconnectedness compared to the types situated on the upper part of this axis. This is evident, for instance, shown by a partial overlap of associational privacy, which is a distinct type in its own right, with certain aspects subordi-

[37] Ibid., p. 557.
[38] MOORE, A. D. *Privacy rights: moral and legal foundations.* University Township: Pennsylvania State University Press, 2011, p. 17.
[39] Or even to satisfy certain natural (en)coding of a human being to realize his or hers own (informational) essence. Cf POLČÁK, R. *Internet a Proměny Práva.* Praha: Auditorium, 2012, pp. 306 and 324. Per the necessity (and tendency) of information spreading cf WANG, D. et al. Information spreading in context. In: *the 20th international conference* [online]. [2023-06-18]. Available at: <http://dx.doi.org/10.1145/1963405.1963508>.
[40] KOOPS, B. J. et al. A Typology of Privacy. p. 501.
[41] RICHARDS, N. M. Intellectual Privacy. *Texas Law Review.* 2008, Vol. 387, No. 87.
[42] See, for example, their explicit link in Article 11 of the Charter Of Fundamental Rights Of The European Union [2000] OJ 364/3.
[43] RICHARDS, N. M. *Intellectual Privacy.* p. 387.

nate to intellectual privacy.[44] Due to this interconnectedness, conducting a separate analysis in the latter half of Koops' typology proves challenging, as a partial idealized analysis would not adequately capture the full scope of the interaction between privacy and automated decision-making.

In relation to intellectual privacy, it is thus appropriate to deal directly with associational privacy as well, which is distancing itself from the intellectual privacy on the horizontal axis of Koops's typology, and thus represents privacy located in the semi-private sphere of individual's life. Associational type of privacy falls within this sphere as it safeguards relationships that occur outside the strictly intimate zone, but still permits, if not requires, a considerable degree of the possibility for exclusion (of others). Essentially, it concerns protecting the freedom of choice regarding with whom an individual will establish connections and share parts of other privacy spheres or types, such as aspects of intellectual privacy, through these connections.[45] Thus, in general, and in conjunction with communicational privacy, it protects a person's natural need to maintain social relations in a broader sense that goes beyond their intimate zone.[46] Given the semi-private nature of this sphere, preserving privacy through the possibility of exclusion becomes more intricate. This is notably manifested in Koops' typology, specifically in its third diagonal axis of *exclusion* from and *control* over information, where associational privacy gradually distances itself from the concept of exclusion.

The type that, according to Koops's typology, relies essentially exclusively on the possibility of control, that is, the subsequent control over information after its disclosure, is behavioural privacy. This type of privacy represents the individual's interest in "being oneself" when engaging in public – in a space from which no one can be excluded merely by the will of the subject.[47] In their final remarks and definitions of the identified types, Koops et al. present two ways in which behavioral privacy, i.e. privacy in a space over which the individual has no control, can be achieved. The first of these approaches shifts the control over access (to space and to information) and internalizes it within the behaving subject - the fulfillment of this privacy may be attained by the individual's efforts to remain inconspicuous in the public space, space over which the subject has no control.[48] However, we hold that such an approach, is in direct contradiction with the essence of this type of privacy, namely in contradiction with the possibility of remaining oneself in this space. Alternatively, the second presented way of achieving (behavioural) privacy in the public

[44] Koops et al. refer, again, to the conception of their typology as ideal types, i.e. types being to a certain extent pure, in the case of intellectual privacy they thus construct a type to be related *ideally* to the privacy of thinking and developing one's own ideas. Even with this ideal conception, however, they themselves point to its strong associational overtones. See the final definitions at KOOPS, B. J. et al. *A Typology of Privacy*. p. 501. In the ideal construction of the typology, Koops refers to Weber's methodology of the social sciences, but it is in relation to this penetration of the other type into, initially, the pure ideal type, not only in the subsequent application observed by Koops (in the first part of the article), but especially by this penetration already inscribed in the pure definition itself, that it can be viewed dialectically, that is, as a Hegelian relation of the always-already contained particularity in the universal, or the universality in each particularity. Cf HEGEL, G. W. F. *Science of logic*. Crows Nest: Allen & Unwin, 1961, para 9.

[45] KOOPS, B. J. et al. *A Typology of Privacy*. p. 568.

[46] Ibid., p. 574.

[47] Ibid., p. 568.

[48] Ibid., p. 568.

sphere is through so called "civil inattention", which in turn shifts the burden of achieving this privacy, as opposed to the approach of inconspicuousness, from a fully internalised mode to a fully externalised one, as it relies on a certain general "social programming" of all participants in the public sphere into "seeing but not noticing" mode.

The final discrete type along this part of the axis is the privacy of decision-making. This takes us back out of the public sphere, since this type refers primarily to decision-making about matters in an individual's intimate sphere.[49] Although this type is sometimes associated with questions of choice in the intimate sphere in a narrower sense, such as questions of the choice of one's partner, the intimate sphere should be understood more broadly, at least to the extent that this sphere constitutes a section of the horizontal axis of Koops's typology. Generally, decisions within this sphere should be viewed, assuming sufficient privacy, as those that an individual can make in accordance with their own convictions, in a state of complete "being as oneself". Similarly, this type is defined by other authors, for example Allen who, as it regards privacy of decision-making, states that it is a protection against (state's) intrusion in the decisions of citizens about the way in which they lead their lives.[50] This conceptualization closely resembles the conventional understanding of meaning behind privacy, or the end goal of protecting privacy through the right to privacy and family life as, for example, articulated in the European Convention on Human Rights. This can be seen, notably, in the ECtHR's interpretation of this concept in the decision Pretty v. the United Kingdom as "the ability to lead a life of one's own choosing".[51]

II.2 Decision making and automated decision making

Having introduced all the, to some extent interrelated, types of privacy targeting the possibility of self-development, or situated in the positive freedom section of the vertical axis of Koops' typology, it is now time to try to identify whether the right not to be subject to automated decision-making can be subsumed under this part of privacy typology. Ultimately, then, it should be a matter of assessing whether automated decision-making in any way interferes with the individual's space of free self-development, or with his or hers *being-as-one-self*.

In order to firmly establish the place of the right not to be the subject of automated decision-making in the legal instruments that aim to protect privacy, it is necessary to classify its place within the typology of privacy. However, such a classification presents complexities that necessitate the establishment of a specific model of automated decision-making, including its scope and the departure points from existing decision-making processes that still retain a substantive "human-in-the-loop" element. The mere removal of the human element without anything else, i.e., essentially perfect virtualization in which the human is a formal element of the process, does not inherently violate the privacy of

[49] Ibid., p. 567.
[50] ALLEN, A. *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press, 2012. p. 4.
[51] *Pretty v United Kingdom* 2346/02 [2002] ECHR 427 European Court of Human Rights. The fact that the issue of euthanasia was at hand in this case demonstrates the need for a broad understanding of the concept of decisions in the intimate sphere of life.

the subject of automated decision-making to a greater extent than that of a standard, non-automated decision-making process. Warren and Brandeis have already argued for the establishment of legitimacy of the intrusion into an individual's privacy in the judicial process,[52] i.e., for the legitimacy of such intrusion in the process of deciding about the rights and obligations of individuals, based on the authority of the state. However, it is not yet possible to conclude solely from this observation that the protection of the subject from automated decision-making has no place in privacy protection-focused legal instruments, or that we should not think of this protection (also) as a privacy protection. If the invasion of privacy is to be facilitated by automated decision-making, and not decision-making as such, the aspect that invades privacy must then be the automation, or the difference that is being represented by the transformation from "normal" human decision-making into the fully automatized one. Given the subject matter of this article and the protective scopes of various types of privacy, in this case the relevant factor is not the lack of human element in the decision making process which usually constitutes the defining element of (fully) automated decision making, but it is rather the technical (and computational) aspect of this approach which allows the decision making process to operate on incomparably greater amount of data.

Given the scope and technical possibilities of automated decision-making, it should then possible to examine, whether this kind of legal regulation is directed at a kind of a self-censorship, i.e. whether it constitutes a direct intrusion into the *intimate sphere* of human being. Automated systems are able, in contrast to human decision-making processes, to consider vast amounts of information in a significantly shorter time, which is made possible, and amplified, by the prevalence of data we currently have on an individual and our unparalleled ability to group them and infer further information from them. For instance, if it is known, that a bank is using geolocation data from smartphones to assess the risk of a loan it is giving to the owner of said smartphone,[53] which means that the bank will also use these data to make a decisions on the fees that individual ought to pay for said loan (and the amount of interest attached to it), will it not affect the places where the individual choose to spend his or hers time, meet with other people and participate in public life (and thus choose to self-censor certain aspects of their life). Such use case extends beyond just banks, which now have unprecedented amounts of (transactional) data from which it is possible to infer a whole range of other substantial information,[54] which can then be used for (automated) decision-making.[55] The automation of some decision-making processes is also gradually emerging in the public sphere, for example in the process of evaluating the fitness for and subsequent allocation of various social welfare benefits.[56] These

[52] WARREN, D. S., BRANDEIS, L. D. *The right to privacy.*

[53] CROSSMAN, P. Would using location data in AI-based credit models improve fairness? In: *American Banker* [online]. 26. 4. 2023 [2023-08-11]. Available at: <www.americanbanker.com/news/would-using-location-data-in-ai-based-credit-models-improve-fairness>.

[54] HOLM, M. Machine learning and spending patterns: A study on the possibility of identifying riskily spending behaviour. In: *KTH, Skolan för datavetenskap och kommunikation* [online]. [2023-08-11]. Available at: <http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-222016>.

[55] This process of inferring and grouping data is known as profiling and it is so intertwined with automated decision making, that legal instruments often address them jointly, even though automated decision making is more akin to a subsequent use of the created (data) profile.

decisions, carried out by the public (administration) bodies, often have a more significant impact on an individual's life than the impact of a decision in the private sphere.[57] Compared to private law decisions, they should thus be made on the basis of much more rigidly established rules, and these decisions must meet a high degree of transparency, both before – meaning that the subject must be made aware of the rules under which the decision will be made, and after, by the clarification of which factors weighed in the decision, which should essentially amount to a properly reasoned judgment/decision.[58]

Thus, public decisions should not afford as much room for excessive or "creative" utilization of big data and various (inferred) datapoints,[59] that have not previously been considered in (human-made) decision-making processes. In this case or even in such case in which the factors considered as relevant for the decision remain unchanged, it is possible to observe the same ingression into the private sphere, demonstrating itself as a certain form of self-censorship, as in the above-described private law decision-making cases. This is namely due to the newly increased capacity to analyze a large amount of data. At this point we have reached a point in privacy protection that partially overlaps with the right to informational self-determination. This intervention becomes particularly relevant when public authorities are tasked with making decisions that involve the assessment of various extra-legal aspects or character traits of the individuals affected, as is the case when determining the suitability of entrusting a child to guardianship, for example.

On one hand, it can be quite validly argued that previous patterns of behavior should be a relevant factor for evaluating character, and especially in such potentially sensitive impactful decisions, such as the decision on placement of the child in care of someone, but it is also important to consider how the "problem of not forgetting" in the digital world, impacts our perception of not only forgiveness,[60] but also our flattening perception of the passage of time, and thus the capacity of a person to undergo personal growth.

The prevalence of automated decision-making may thus represent an unprecedented invasion of human privacy precisely through a significant reduction of the intimate sphere, where one must consider the possible impact on the subsequently inferred pattern of behaviour, even for decisions made in the previously isolated intimate sphere. The sphere in which the individual can be oneself and *by-oneself* alone will thus be considerably reduced. What speaks more to the necessity of a proper regulation and establishment of rules for these automated processes is that such individual data points and instances of past behaviour may in the end never even be relevant for the (automated)

[56] HEIKKILÄ, M. Dutch scandal serves as a warning for Europe over risks of using algorithms. In: *POLITICO* [online]. [2023-06-11]. Available at <www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>.

[57] The article cited in the previous note about the error in social welfare decision-making in the Netherlands, itself directly in the lead, speaks of the *destruction* of thousands of lives.

[58] KRIŠTOFÍK, A. Právo na odôvodnené rozhodnutie a algoritmizácia rozhodovacích systémov. *Právník*. 2023, Vol. 162, No 1. pp. 39–48.

[59] Such approach would essentially constitute a massive surveillance program of citizens, or such totalization of behavior and decision-making is only one step away from it, and to some extent, this aspect is also what the various privacy protection tools are aimed at. Cf QIAN, I. et al. Four Takeaways from a Times Investigation into China's Expanding Surveillance State. In: *The New York Times* [online]. 21. 6. 2022 [2023-08-11]. Available at: <https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html>.

[60] POLČÁK, R. *Internet a Proměny Práva*. pp. 300–341.

decision-making process, but due to the low level of transparency, and our almost technically inherent impossibility of knowing these processes,[61] or the reluctance of the developers to open up the "hood" of these systems,[62] it will be treated as possibly relevant and decisive aspect for (any possible) future decision, thus interfering with the (decisional) privacy,[63] if not properly regulated

At this point, a discernible encroachment upon the individual's (decisional) privacy becomes evident., since the individual, as a (possible future) subject of an automated decision-making, is no longer afforded the opportunity to carry intimate decisions of his or her own volition without third-party interference. The example of banks employing geolocation data to make loan decisions highlights how this process compromises the individual's full exercise of associational privacy at the same time, and further it is equally questionable to what extent such self-censorship also interferes with the individual's intellectual privacy.[64]

More broadly, one can thus also observe the interaction of such automated decision-making with the general concept of privacy and its purpose as introduced above, that is, its interference with the ability to lead a life of one's own choosing. It goes without saying that the individual, as part of human society, is not absolutely free to make decisions about how to lead his or her own life; this constraint is, in a sense, a constitutive element of human society. However, it is precisely for this reason that in order to preserve the individuality of the individual in society, or to preserve human society as a singularity of individuals, it is necessary to preserve the intimate sphere of the individual and to protect the decisions he or she makes in it to the greatest extent possible, against its further narrowing by the totalization of the digital non-forgetting.

Precisely in view of the fact that the individual needs to be regarded as an integral part of society, as well as individual's inherent need for self-development (as elucidated by the previously discussed group of privacy types) depends to a large extent on the possibility

[61] Such situation should also open up the possibility for discussion about the effects of these impacts in the braoder picture of the (current) societal changes, or to be more precise, discussions about the complementarity of such incursion into the (very intimate) privacy of the individual with the various theories of power (demonstration) in and over the society as a whole. As we have seen the Foucault's biopolitical power over the subject represented by the shift to regulation, the society controlled/governed by algorithms and self-censorship is often described as psychopiltics. This shift in the demonstration of power in the society is defined precisely by the influence it exerts over the psyché, generally seen in the shift from the subject to project and is made possible precisely by the adoption of the new technologies by the current biopower. Cf HAN, B. *Psychopolitics: Neoliberalism and New Technologies of Power.* New York: Verso, 2017. For an analysis of the transition from a Foucaltian conception of power, cf LANDÁZURI, M. C. O. From Biopolitics to Psychopolitics in Byung-Chul Han's social thought. In: *Athenea Digital* [online]. [2023-08-12] Available at: <http://dx.doi.org/10.5565/rev/athenea.1782>.

[62] LIU, H. et al. Beyond State v Loomis: artificial intelligence, government algorithmization and accountability. *International Journal of Law and Information Technology.* 2019, Vol. 27, No. 2. p. 122.

[63] An ad absurdum approach can thus liken this situation to the posthumanist thought experiment of "Roko's Basilisk", which essentially posits to the subject of this experiment that he should start behaving at this moment according to the rules of a hypothetical non-existent artificial intelligence system, as precisely because for the capacity of these systems to work with historical data, this is the only rational option.

[64] It is precisely to the intellectual privacy of the individual that we currently have unprecedented and practically unexpectedly intensive access, as shown, for example, by the case related to the activities of Cambridge Analytica on the social network Facebook. Cf CONFESSORE, N. Cambridge Analytica and Facebook: The Scandal and the Fallout so Far. In: *The New York Times* [online]. 4. 4. 2018 [2023-08-21]. Available at: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

to communicate and receive information about oneself and other members of society, it is also possible to conclude that protection against automated decision-making must be seen as a right of control over the information that has already been disclosed. Contrary to viewing it solely within the context of privacy as an exclusive claim, this perspective acknowledges the significance of communication and information exchange for the individual's growth and societal integration. Koops himself gravitates towards a similar outlook in his subsequent work on ambient intelligence, where he redefines the legal perception of data concerning an individual and their rights to such data. In this work concept of "smart regulation" of information privacy is introduced, which surpasses mere data concealment and emphasizes the creation of a space that enables the individual to specifically control the disclosure of data in response to varying situations and information received, thus essentially empowering individuals with control over their disclosed data.[65]

The final, and practically ancillary, step in the examination of Koops's typology is to consider the last, ninth, type – the informational privacy. This type, by its very nature, intersects with all the other types, and as a result, after having identified the appropriate classification for the right not to be subject of automated decision-making (which also overlaps with several types), it becomes evident that this right can be encompassed within the realm of informational privacy. This type of privacy, according to Koops et al., consists in the individual's ability to control, or prevent, the collection of information concerning him or her self.[66] Not only because of the overlap of this type with other types of privacy, under which we could subsume the right not to be the subject of automated decision-making, but also because we have identified this right to embody the characteristics of *control-based* types of privacy – which are such types of privacy primarily intended to ensure the (space for) self-development and autonomy of an individual[67] – the informational (privacy) aspect of this right becomes quiet evident.

II.3 Protection of autonomy and dignity as a base for the right to not be subject of automated decision making

The protection of privacy within the various legal instruments often does not exist for its own sake but has the ultimate purpose of protecting another legally relevant value(s). As observed above, the protection of privacy, or at least the positive aspects of it – the *freedom to* - combined with the concept of privacy protection as the concept of *control* over information, should lead ultimately to the protection of the autonomy of the individual. The aspect of protection of one's autonomy is most evident in the general conception of privacy as the ability to make free choices and decisions about the way in which an individual conducts his or her own life – it inherently embodies precisely the autonomy over one's own existence.

Thus, if we were not to conclude that the right not to be the subject of automated decision-making can be subsumed under one of the types of privacy identified by Koops, it

[65] HILDEBRANDT, M., KOOPS, B. J. The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review.* 2010, Vol. 73, No. 3. pp. 428–460.
[66] KOOPS, B. J. et al. *A Typology of Privacy.* p. 568.
[67] Ibid., p. 559.

would be necessary to look further for a reason, or purpose, for the inclusion of this right in the provisions, or instruments, that are primarily designed to protect privacy.

In the pursuit of identifying additional values that may be represented and protected by privacy-related instruments, or in some way inherently shape privacy and its purposes in our society, we can draw insights from Koops himself in his typology. In his own introductory conceptualization of privacy and the right to privacy, he highlights its "strong links to extra-legal conceptualizations of privacy, such as freedom, individuality, autonomy, personhood, and human dignity".[68] The intersection between privacy and these other concepts to which privacy is supposed to be closely related to is also further explored by Koops et al. in their subsequent analysis of various constitutional orders, wherein they trace some of these elements, including the concept of human dignity found in the German constitutional order and its conceptualization of the right to informational self-determination (and thus informational privacy)[69]. The idea that these concepts may overlap with the right not to be the subject of automated decision-making is supported by the fact that in the previous section we identified this right as a manifestation of the aspect of control, which serves as the basis for and the instrument of, privacy, to which, according to Koops, these aspects identified in constitutional orders are equally directed towards.

The concept of autonomy finds expression in various aspects related to automated decision-making. For instance, the concept of autonomy manifests itself in the requirement to be informed about the underlying logic of such decisions,[70] which is closely tied to the concept of the right to a fair trial, as it enables the possibility of appealing against a decision.[71] This is essentially closely followed by the very preservation of the possibility of the human element intervening[72] into the process, which is meant to be aimed at preserving the dignity of the subject, by respecting and retaining the human agency.[73] Each of these factors, however, is in itself such a fundamental issue in automated decision making that it is possible, and desirable, to consider them outside of their relationship to the concept of privacy. At the same time, all of these questions bring us back to the beginning of this article, or rather, they are questions essential to (preserving) the anthropocentricity of law.[74]

III. CONCLUSION

The primary objective of this article was to determine the place of the right not to be the subject of automated decision-making within the framework of legal instruments pro-

[68] Ibid., p. 493.
[69] Ibid., p. 562.
[70] Cf Art. 22 of GDPR.
[71] JACKSON, J. Autonomy and Accuracy in the Development of Fair Trial Rights. In: *SSRN Electronic Journal* [online]. [2023-08-11]. Available at: <http://dx.doi.org/10.2139/ssrn.1407968>.
[72] HUQ, A. Z. A Right To A Human Decision. *Virginia Law Review.* 2020, Vol. 106, No. 3, pp. 611–688.
[73] Alan Rubel and others, Algorithms, Bias, and the Importance of Agency. *CEUR proceedings* 21(1). In: *ceur-ws.org* [online]. [2024-04-18]. Available at: <https://ceur-ws.org/Vol-2103/paper_2.pdf>.
[74] For this, cf, e.g., BELOV, M. Post-human Constitutionalism? A Critical Defence of Anthropocentric and Humanist Traditions in Algorithmic Society. In BELOV, M. *IT Revolution and Its Impact on State, Constitutionalism and Public Law.* Bloomsbury Publishing Plc, 2021. pp. 15–40.

tecting privacy, by classifying this right within one of the 8+1 types of privacy conceptualized by Koops et al. The classification itself under a specific (ideal) type of privacy is not completely straightforward, partly precisely because of their ideal nature. However, a closer examination of Koops et al.'s dimensions defining each type of privacy reveals that the right not to be the subject of automated decision-making is fundamentally a right of control. Its purpose is to protect the individual's privacy space, providing them the freedom to shape their life according to their own preferences, thus indicating a concept of privacy as a realm for self-development.

Evidently, the right not to be the subject of automated decision-making is positioned at the intersection of several types within Koops' typology, specifically decisional, associative, and intellectual privacy. A critical factor in determining the potential impact of any automated decision-making process on an individual's privacy lies in the technical approach to automation and the subsequent handling of data.[75] It is crucial to consider whether the automation merely involves algorithmizing existing processes without any modifications, as this should not significantly affect privacy beyond what human-made decisions already do.

However, it is also possible to view this right in the context of other privacy-related aspects that this right equally tends towards, such as the protection of human dignity and human agency, or the protection of human autonomy, as concepts that are not only closely related to the concept of privacy but also to the fundamental Kantian principle of the anthropocentricity of law, the analysis of which is all the more relevant in the ever-expanding post-humanistic algorithmic society.

[75] As to the need for defining and differentiating between various AI models and approaches for the discussion on (public) data use in automated decision making and its impact on privacy cf Holms' response to aforementioned Plougs' article (Ploug n 13) in HOLM, S. Should People Have a Right Not to Be Subjected to AI Profiling based on Publicly Available Data? A Comment on Ploug. *Philosophy & Technology.* 2023, Vol. 36, No. 2.