Collection of Papers
from the International Academic Conference
12 – 13 September 2022

LEGAL CHALLENGES OF AUTOMATED WORLD

BLF BRATISLAVA LEGAL FORUM 2022

Zborník príspevkov
z medzinárodnej vedeckej konferencie
12. a 13. septembra 2022

BPF BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2022

SYMPÓZIÁ, KOLOKVIÁ, KONFERENCIE

LEGAL CHALLENGES OF AUTOMATED WORLD

BRATISLAVA LEGAL FORUM 2022

BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2022

Collection of Papers from the International Academic Conference
Bratislava Legal Forum 2022
organised by the Comenius University in Bratislava, Faculty of Law
on 12 – 13 September 2022
under the auspices of the Alumni Club of Comenius University in Bratislava, Faculty of Law.

Zborník príspevkov z medzinárodnej vedeckej konferencie
Bratislavské právnické fórum 2022
organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou
v dňoch 12. – 13. septembra 2022
pod záštitou
Alumni Klubu Univerzity Komenského v Bratislave, Právnickej fakulty.

Univerzita Komenského v Bratislave
Právnická fakulta
2022

Editors / Zostavovatelia:

- Mgr. Michaela Durec Kahounová
- Mgr. Silvia Senková

Všetky príspevky prešli dvojitým anonymným recenzným konaním.

ISBN 978-80-7160-666-6
EAN 9788071606666

CONTENT / OBSAH

DATA SUBJECTS' RIGHT TO ACCESS INFORMATION RELATING TO THE RECIPIENTS TO WHOM THE PERSONAL DATA HAVE BEEN DISCLOSED: LEGAL CONTROVERSIES

Juanita Goicovici

University Babeș-Bolyai of Cluj-Napoca, Faculty of Law

Abstract: The paper discusses the problematics of the data subjects' right to access information relating to the recipients to whom the personal data have been disclosed under the provisions of Article 15, 1st para., let. c), corroborated with Article 19 of GDPR, accentuating the legal controversies contoured around the limits of the exercise of the mentioned right. Firstly, the study focuses on the legal dilemmas entangled by the substantial limits of the exercising of data subject's right to access information on data processing, deciphering the provisions of Article 15, para. (1), (c) of the GDPR, according to which the data subject has the right to access information relating to the recipients or categories of recipient to whom the personal data have been disclosed, particularly recipients in third countries or international organizations. Secondly, the accent is placed on the importance of the provisions of Article 19 of the GDPR which require the data controller to inform all recipients to whom it has transferred personal data of any request for the rectification, erasure, or restriction of processing of those data with which the controller has an obligation to comply.

Key words: data subjects, right of access, GDPR, personal data, data controller's obligations, data recipients.

1 INTRODUCTION

Situated at the core of the legal protection allocated to data subjects in terms of exercising their prerogatives of control over the processing and transferring of personal data, the problematics of the data subjects' right to access information relating to the recipients to whom the personal data have been disclosed under the provisions of Article 15, 1st para., let. c), corroborated with Article 19 of GDPR, have been marked by multiple legal controversies, which were contoured around the limits of the exercise of the mentioned right. Firstly, the study focuses on the legal dilemmas entangled by the substantial limits of the exercising of data subject's right to access information on data processing, deciphering the provisions of Article 15, para. (1), (c) of the GDPR, according to which the data subject has the right to access information relating to the recipients or categories of recipient to whom the personal data have been disclosed, particularly recipients in third countries or international organizations. Secondly, the accent is placed on the importance of the provisions of Article 19 of the GDPR which require the data controller to inform all recipients to whom it has transferred personal data of any request for the rectification, erasure, or restriction of processing[1] of those data with which the controller has an obligation to comply. In this context, recipients so informed are subsequently required to immediately rectify (under reasonable time bars), erase, or restrict the processing of personal data, upon data subject's request.

Thirdly, the paper emphasizes the idea that, in pursuit of the objective of ensuring a high level of protection, as mentioned in CJEU Advocate General's Opinion in Case C-154/21[2], the provisions of Article 19 of the GDPR are "intended to relieve data subjects who have requested information pursuant to Article 15(1)(c) of the GDPR of the burden of sending further corresponding requests for

[1] SWIRE, P. When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer, p. 21; VOSS, W. G. European Union Data Privacy Law Reform: General Data Protection Regulation (...), 2017, p. 226.

[2] The CJEU Advocate General's Opinion in Case C-154/21 is available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=260543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=183615.

rectification, erasure or restriction of processing to the recipients concerned" and that, nonetheless, the data subject must be enabled to exercise legal prerogatives[3] permitting to verify that the data rectification, erasure or restriction has been adequately carried out by third parties / controllers following notification by the initial data controller. We argue that the provisions of Article 19 of the GDPR may be interpreted in the sense that those provisions are providing that the data controller must inform the data subject on the identity of third-party recipients of personal data. Bifurcated into data subject's right to exercise control over personal data collecting and processing based on a granular consent (i) and data subjects' right to access sufficient information on third-party data controllers, the legal prerogative described in Article 15 and 19 of GDPR imbricates a plurality of legal valences. We argue that an interpretation favoring an object-restrictive view on data subjects' right to access information on the identity of data recipients to whom their personal data have been previously disclosed would have the consequence of diluting data subjects' right of control over data processing, since the latter would not be in a position to exercise against subsequent data recipients engaging in sequential data collecting and processing, the rights to data portability, 'right to be forgotten', data access and data control (rectification, erasure, restriction of processing) conferred on data subjects by the abovementioned provisions of the GDPR or would be able to exercise those rights only by engaging in a disproportionate effort.

Finally, we argue that an antagonistic interpretation (on restricting data subjects' right to access information on the categories of recipients) would collide with the exigencies of the principle of effectiveness of EU Law. Although the wording and phrasing of Article 15, para. (1), let. (c) of the GDPR does not enable a categorical answer to be given to the practical interrogation of whether the data subject's right of access must necessarily be regarded as extending to access to information regarding specific recipients to whom personal data concerning the data subject has been disclosed, or whether it might be limited to access to information merely regarding categories of recipients, we conclude that, in terms of ensuring transparency of data processing, in the hypotheses in which the disclosure of data recipient's identity upon data subject's request remains possible on no exceptional costs or insurmountable difficulties for the initial data controller, the latter should have an obligation to provide the data subject with this set of information[4], exceeding the mere indication of the category of recipients to which personal data has been previously disclosed.

2 ACCESSING INFORMATION ON PERSONAL DATA RECIPIENTS: MAIN TRAITS

2.1 Objective components of the data subjects' right to access information

The right of access information relating to the recipients to whom the personal data have been disclosed includes three different components: (i) confirmation as to whether data about the person is processed or not based on a transfer to third-party recipients; (ii) instructions concerning the manner of access to third-parties processed personal data; (iii) access to information on the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third-country transfers. Especially, it is worth recalling that, pursuant to Article 15(1) of the GDPR, the data subject has the right to obtain from the controller confirmation as to whether personal data concerning the data subject are being processed and, in the hypotheses in which an affirmative answer has been issued on the fact that such data are being processed, the data subject has the right to access the personal data that are being processed, as well as certain further information, listed in points (a) to (h) of that provision. Nonetheless, pursuant to the provisions of Article 15, para. (1)(c) of the GDPR, the data subject has the right to access information relating to

[3] BRÄUTIGAM, T. The Land of Confusion: International Data Transfers between Schrems and the GDPR, p. 87; CHRISTAKIS, T. Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?, p. 31; CORRALES COMPAGNUCCI, M., ABOY, M. and MINSSEN, T. Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses, p. 2.

[4] DI PORTO F., GROTE T. and VOLPI, G. Talking at Cross Purposes? A computational analysis of the debate on informational duties in the digital services and the digital markets acts, pp. 87-89.

'the recipients or categories of recipient' to whom the personal data have been or will be disclosed the recipients in third countries or international organizations[5].

It must be pointed out that recital 63 of the GDPR expressly states that data subjects should be recognized the right obtain details regarding the recipients of the personal data, in the hypotheses in which such a transfer took place. Consequently, the recital 63, in the light of which the provisions of Article 15 of the GDPR must be interpreted, relates the data subject's right of access to the specific recipients to whom personal data are disclosed; more importantly, the provisions of Article 15 do not mention restrictions at the data controller's discretion, merely to specifying the categories of recipients the identity of whom to be disclosed to the applicant when exercising the latter's right to access information on data recipients.

Secondly, it is also worth recalling that, at the core of the purpose of the GDPR provisions is, as recital 10 makes transparent, the desiderate of ensuring a high level of protection of data subjects within the European Union and, more extensively, of ensuring a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data, including in cases in which these data are subject to transferring to third-party recipients, even for those recipients who were situated outside the EU territorial boundaries. It is therefore conjunctive and concerted to the mentioned purposes that any processing of personal data must comply with the principles set out in Article 5 of the GDPR, since it is particularly central, as resulting from the provisions of Article 5, para. (1)(a) of the GDPR that personal data are processed in a transparent manner in relation to the data subject, thus enabling the latter to access specific information the knowledge of which remains essential for the exercising of the prerogatives of control over data processing and transferring[6]. Contextually, from the provisions of Article 15 of the GDPR, which governs the data subject's right of access, it results that the stipulating of the data subjects' right to access information constitutes a central provision for ensuring that the specific manner according to which data are processed conserves its transparency in relation to data subjects[7].

Congruently to the previously mentioned assertions, it remains essential to note that, as resulting from the description included in recital 63 of the GDPR, the purpose of the right of access finds its pillars in the desiderate to enable the data subject with concrete and efficient prerogatives of control, meant to verify the lawfulness of the data processing[8]; therefore, the at the very core of the exercising of the right to access information on data recipients lies the rationale of enabling the data subject to verify not only the accuracy of the content which concerns processed personal data, but also to check on the manner in which these data are or have been disclosed to (un)authorized recipients, based on the information provided by the initial data controller, which is expected to be as precise and accurate as technically and legally possible.

2.2 Prerequisites of consent-collecting to personal data processing and transferring

When assessing whether consent to the processing of personal data is freely given, utmost account would be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract[9]. The key point is that consent to data processing must be opt-in consent, implying a positive action or indication, since there is no valid 'opt-out consent' to data processing recognized by the legal provisions. Particularly, it must be pointed out that data subject's failure to opt out is not considered to be consent as it does not involve a clear affirmative act.

Therefore, when collecting data subjects' consent to a specific taxonomy of processing operations, data controllers may not rely on silence, inactivity, default settings, pre-ticked boxes or general terms and conditions, nor are data controllers allowed to seek taking advantage of consumers'

[5] JURCYS, P., CORRALES COMPAGNUCCI, M. and FENWICK, M. The future of international data transfers: managing legal risk with a 'user-held' data model, p. 4.
[6] MAHIEU, R. The right of access to personal data: A genealogy, 2021, p. 62.
[7] *Ibidem*.
[8] GOICOVICI, J., Dreptul relațiilor dintre profesioniști și consumatori, 2022, p. 56.
[9] GOICOVICI, J. Consimțământul consumatorului la prelucrarea datelor personale în contractele business to consumer – condiția consimțământului granular, 2019, p. 17.

inertia, users' inattention, or default bias. Nevertheless, certain consent-collecting methods also involve ambiguity entangling inefficiency of consent: for data subject's consent to be valid it must be both unambiguous and affirmative[10]. It must be clear that the individual deliberately and actively chose to consent to personal data processing, since implicit agreeing or tacit consenting is not recognized as presenting legal validity. The requiring for an affirmative act does still imply difficulties for the implementing of implied methods of consent collecting in certain B2C contractual circumstances, particularly in more informal offline or online contracting situations. The key issue remains that there must still be a positive action that makes it clear that data subject is agreeing to the use of their information for the engaging in data processing activities for a specific and obviously described purpose. However, this type of implied method of indicating consent would not extend beyond what was obvious and necessary purpose of data processing, as it remains essential to underline that clear affirmative action means consumers must take deliberate and specific action to opt in or agree to the processing, even if this is not expressed as an opt-in box. For example, other affirmative opt-in methods of consent collecting might include signing a consent statement, verbal confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default.

Particularly, it should be emphasized that data subjects must be able to refuse consent without detriment, and must be able to withdraw consent easily at any stage of data processing[11]. It also means consent should be unbundled from the remaining contractual terms and conditions (including giving separate granular consent options for different types of processing) wherever possible. Even if the new purpose of data processing is considered 'compatible' with the original purpose of personal data processing, the compliance to this requirement does not override the need for data subject's consent to be specific; thus, in situations where the collecting and processing of personal data were based on the existence of the consumer's consent, the 'stratification' of the purposes of personal data processing, as well as the 'stratification' of consent-collecting for each type of processing operation represent special requirements arising from the condition of granular consent, which is why a consent requested in general terms will not be valid, 'for any personal data processing operations' or for the so-called 'purposes related to the execution of the contract', without an explicit statement and distinct of each of the purposes of data processing (the so-called 'sequencing of the purposes of processing'). If professional traders were relying on consumers' consent, the former therefore need to either obtain the data subject's specific consent, or else identify a distinctive lawful basis for the evolving purpose of data processing[12].

Nonetheless, should the consumer object to the processing for the purpose of direct marketing, the processing of personal data cease to be covered by the initially-collected consent (which remains essentially revocable). In the cases where the processing of personal data for direct marketing purposes is mentioned in standard B2C contractual terms, to the extent that this clause 'conditions the conclusion of the contract on the expression of consent to the future permission to use personal data in order to put in practice of marketing directed at the targeted person, then such a clause must be considered abusive or directly invalid', which represents a justified solution, through the prismatic purpose of repressing the probable lack of transparency and the creation of an immediate imbalance between the rights and obligations of the parties, to the detriment of the data subject.

[10] KAISER, E. The Concept of 'Freely Given, Specific and Informed' Consent (...), p. 608.
[11] KE, T. and SUDHIR, K. Privacy Rights and Data Security: GDPR and Personal Data Markets, p. 3; KUNER, Ch. Territorial Scope and Data Transfer Rules in the GDPR (...), p. 2; LEISTNER, M.: The Existing European IP Rights System and the Data Economy (...), p. 12; LEONARD P. Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing (...), p. 4.
[12] GOICOVICI, J. Dreptul relațiilor dintre profesioniști și consumatori, 2022, p. 37; JAROVSCY, L. Improving Consent in Information Privacy (...), p. 449; JASMONTAITE, L., KAMARA, I., ZANFIR-FROTUNA, G. and LEUCCI, S. Data Protection by Design and by Default. p. 168.

2.3 Adequacy assessments and the importance of implementing appropriate safeguards for data transferring

Previous scholars have underlined the importance of implementing adequate safeguards[13] in the hypotheses in which personal data are transferred to third-party recipients; it has been emphasized in specialized literature that: „*Adequacy decisions are based on assessments that third country laws and practices guarantee the same level of European standard protection. The effect of such decisions is that personal data can flow without restrictions and any further additional safeguards. In other words, transfers to the countries in this list will be assimilated to intra-EU transmissions of data.*"[14] The adopting of appropriate safeguards is envisaged under the provisions of Article 46 of the GDPR; previous scholarly work anticipated that: „*In the absence of adequacy decisions, organizations involved in the cross-border transfers must implement 'appropriate safeguards' (i.e., Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), codes of conducts, certification mechanisms and ad hoc contractual clauses) to ensure that the level of protection is not undermined*"[15]. It has also been stressed that "*the CJEU developed and uses as a benchmark 'essential equivalence' both as a standard to achieve but also as a fundamental rights test for destinations of data transfers to pass."*[16]

3 REVERBERATIONS OF THE EXERCISE OF DATA SUBJECTS'S RIGHT TO ACCESS INFORMATION

Under the facets of the consequences of exercising the right to data portability[17], posteriorly to the establishing of the existence of the right of the data subject to take control over the processing and transferring of personal data[18], the obvious question (with less obvious answers) refers to outlining several clear benchmarks regarding what the actual exercise of the mentioned right. Pursuant to the provisions of Article 20 of the GDPR, the data subject has the right to receive personal data in a structured format, that is currently used and which can be read automatically (access which, as it has been specified in precedent paragraphs, is expected to be issued within one month from the receiving of the data subject's request, according to the provisions of Article 12, para. (3) of the GDPR)[19]. Sequentially, the prerequisites mentioned in the text of Article 20 of the GDPR refer to the fact that the data controller is expected to be able to provide for a structured set of data presenting the attributes allowing it to be considered, from a technical point of view, a portable set of personal data. In cases where it is technically feasible, the data subject may request the data controller to transmit processed data in a non-intermediate manner, directly to another data controller, specifying that both the reception and transmission of personal data can be requested at any time of data processing (prior to possible anonymization), as being, in principle, exercised in a non-onerous manner (with the exception of reasonable costs which can be charged for honoring repetitive access / porting requests formulated by the respective data subject on recurrent intervals).

Recognizable by the fact that, particularly, the personal data the transferring of which is requested are placed in interconnectivity with the personal data of other data subjects[20], a salient exception to the personal data portability rule intervenes in the event when the data subject's request

---

[13] DRECHSLER, L. and KAMARA, I. Essential Equivalence as a Benchmark for International Data Transfers After Schrems II, 2021, p. 4; DRECHSLER, L. What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights, p. 3; GOICOVICI, J. Clauzele privind drepturile consumatorilor în contractele de servicii cloud computing, p. 399.

[14] See CORRALES COMPAGNUCCI, M., ABOY, M. and MINSSEN, T., *op. cit.,* p. 2.

[15] *Ibidem*.

[16] DRECHSLER, L. and KAMARA, I. Essential Equivalence as a Benchmark for International Data Transfers After Schrems II, 2021, p. 2.

[17] GOICOVICI, J. Portabilitatea datelor cu caracter personal, prin prisma dispozițiilor RGDP (...), p. 58.

[18] *Idem*, p. 62.

[19] LUNDQUIST, B. An Access and Portability Right to Data (...), 2022, p. 3.

[20] LUNDQUIST, B. Big Data, Open Data, Privacy Regulations (...), 2018, p. 192; LUZAK, J. Digital age: time to say goodbye to traditional concepts, 2018, p. 23; MAHIEU, R. The right of access to personal data: A genealogy, 2021, p. 62.

were admitted, the infringing of the rights of third-parties would be involved, at least, in a manner which is inadequate to the reasonable expectations of the other concerned persons involved. In the latter case, exercising the right to data portability cannot be accommodated with the control prerogatives belonging to other involved persons, which imposes, as an undeniable consequence, the legitimate refusal of the operator to comply with the request for access or data transferring[21].

As it has been previously observed in specialized literature[22], the data subjects' right of access is central to the enabling of data subjects to exercise a plethora of adjacent rights, such as the right to data rectification, the right to obtain data erasure (including the 'right to be forgotten') and the right to obtain restriction of processing, conferred on data subjects by Articles 16, 17 and 18 of the GDPR. Respectively, in accordance with Articles 79 and 82 of the GDPR, the right of access is also necessary to enable data subjects to object to the processing of their personal data, as provided for by Article 21 of the GDPR, and to subsequently take legal action in order to obtain compensation in the event when data processing and transferring was able to cause harm or had prejudicial effects.

Therefore, it must be emphasized that the exercise of the right to access information on the recipients of personal data does not generate merely insular effects, yet implying a plurality of reverberations; particularly, an interpretation of the provisions of Article 21 of the GDPR according to which data subjects could not obtain information regarding the specific recipients to whom their personal data are disclosed would have the consequence that, 'ignorant of the identities of such recipients, data subjects would not be in a position to exercise against them the rights conferred on them by the abovementioned provisions of the GDPR or would be able to exercise those rights only by making a disproportionate effort'[23]. Such an interpretation seems to remain essential for describing the tributaries and the plurality of valences attributable to the data subject's right to access information on the identity of data recipients, without depriving those provisions of Article 15, 1st para. of the GDPR, and the rights which they confer to data subjects, of their effectiveness in situations of this type.

Eloquently and from a contextual perspective, it must also be stressed that the coordinates of the abovementioned interpretation of Article 15, para. (1)(c) of the GDPR seem to be interconnected to the provisions of Article 19 of GDPR, the provisions of which state that '*the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort'*. From the second thesis of Article 19 of the GDPR, corroborated with the mentioned provisions of Article 15, para. (1)(c) of the GDPR, it results that the protectionist mechanism described by the GDPR provisions requires the data controller to inform all recipients to whom it has transferred personal data of any request received form the data subjects for the rectification, erasure, or restriction of processing of those data with which the initial data controller, as well as the subsequent or tertiary controllers must comply. It also results, as a direct consequence of the exercising of data subjects right of access and to obtain data erasure or data rectification, that recipients so informed are, posterior to the informing on the admittance of the data subject's request, required immediately to rectify, erase, or restrict the processing of the personal data, obviously to the extent that they are still processing these data. As it was rightly pointed out, the trend of 'convergence' of the person's right to private life (a) and the data subject's right to the protection of personal data (b), on the other hand, are justified by the fact that the mechanism of protection of personal data respects the desire to preserve private life, also functioning as a foundation for a suite of concrete rights, such as the right to control over personal data, the right of access to the personal data the respect of which is incumbent on data controllers, as well as the right to oppose the processing of personal data, the right to withdrawal of consent to data processing and the right to portability of personal data.

Consequently, it should be emphasized that in pursuit of the objective of ensuring a high level of protection, mentioned in Article 19 of the GDPR, the latter's provisions are intended to 'relieve

[21] RUBINSTEIN, I. and MARGUILIES, P. Risk and Rights in Transatlantic Data Transfers (...), 2021, p. 3; SWIRE, P. and KENNEDY-MAYO, D. The Effects of Data Localization on Cybersecurity, 2022, p. 4.
[22] VOSS, W. G. European Union Data Privacy Law Reform (...), 2017, p. 226.
[23] See the CJEU Advocate General's Opinion in Case C-154/21, *loc. cit. supra.*

data subjects who have requested information pursuant to Article 15, para. (1)(c) of the GDPR of the burden of sending further corresponding requests for rectification, erasure, or restriction of processing to the recipients concerned'[24]. Nonetheless, the data subject must be facilitated the ability to verify, posterior to the admission of the request, whether the rectification, erasure or restriction has actually been carried out following notification by the subsequent or tertiary data controller, since Article 19 of the GDPR therefore provides that the data controller must inform the data subject of those recipients should the data subject request for the providing of specific information on third-party recipients of personal data.

4 CONCLUSIVE REMARKS

Saliently, the data subjects' right to access information relating to the recipients to whom the personal data have been disclosed under the provisions of Article 15, 1st para., let. c), corroborated with Article 19 of GDPR entangled a series of legal dilemmas concerning the substantial limits of the exercising of data subject's right to access information on data processing and to the deciphering the provisions of Article 15, para. (1), (c) of the GDPR, according to which the data subject has the right to access information relating to the recipients or categories of recipient to whom the personal data have been disclosed, particularly recipients in third countries or international organizations. Although the definitory traits and the material sphere of the right to access information are far from being monolithically described, the prerequisites of the exercising of the right of access are based on the provisions of Article 19 of the GDPR, which require the data controller to inform all recipients to whom it has transferred personal data of any request for the rectification, erasure, or restriction of processing of those data with which the controller has an obligation to comply.

Placed under a double limit, which allows the prerogative of data accessing to substantially contribute to the exercising of the data subject's right to obtain data portability, the right to obtain information on data recipients allows data subjects to exceed the subjacent role under which the scope of personal data portability is restricted, firstly, from a subjective point of view and, at the same time, objectively, since portability concerns the personal data belonging to the concerned person; the consent to the processing of the personal data was voluntarily provided by the data subject to the initial data controller, requiring the collecting of an opting-in consent, which can later be withdrawn at any stage of data processing (except for the hypotheses in which further processing of personal data, after the consent withdrawal, remains necessary for the performance of the obligations resulting from a B2C contract currently being executed). The person responsible for the processing has the obligation to comply and to transmit the data requested, thus being able to configure the architecture of this right to obtain information on third-party recipients of personal data, as an expression of the prerogatives of the person concerning the withdrawal of previously-collected consent to data processing. On the other versant of the discussion, the right to consent withdrawal to the processing of personal data, which would be essential for consent-based processing in the contextual interpretation of the GDPR provisions, encapsulates the mentioned prerogatives of the data subject to request and obtain, as specifically as possible, the recovery of the set of personal data (which were transmitted, actively and consciously, by the previous operator to subsequent recipients, as well as the collected data resulting from the subject's activities), in a format which would allow their reuse (especially in terms of data portability and data rectification).

Subsequently, on the other hand, in situations where the processing of the consumer's personal data is aimed at direct marketing, the data subject has the right to object at any time to the processing for this purpose of the personal data concerning the data subject's preferences, including the profiling activities, insofar as it is related to direct marketing operations. We noted that, if the consumer objects to the processing for the purpose of direct marketing, the personal data can no longer be processed for this purpose. In the cases where the processing of personal data for direct marketing purposes is mentioned in a standard B2C clause, to the extent that this clause 'conditions the conclusion of the contract on the expression of consent to the future permission to use personal data in order to put in practice of marketing directed at the targeted person, then such a clause must be considered abusive or directly invalid', which represents a justified solution, through the prismatic purpose of repressing the probable lack of transparency and the creation of an immediate imbalance

[24] The CJEU Advocate General's Opinion in Case C-154/21, cit. supra, pt. 24.

between the rights and obligations of the parties, to the detriment of the consumer, in the latter's quality of data subject.

Thirdly, the control that the data subject can exercise over personal data collected by the initial data controller depends to a decisive extent on the latter's compliance with the principle of transparency, according to which data operators must ensure that any information and communications concerning the processing and further transferring of personal data are easily accessible and communicated upon the data subject's request in a comprehensible manner and that plain language is used. The transparency principle refers in particular to informing the data subjects regarding the identity of the secondary, tertiary or subsequent data controllers and on the purposes of the processing, as well as to the providing of additional information, in order to ensure a fair and transparent processing with regard to the natural persons concerned and their right to be informed on the recipients of the personal data which have been transferred upon the initial data controller's initiatives.

Bibliography:

BRÄUTIGAM, T: The Land of Confusion: International Data Transfers between Schrems and the GDPR, In: T. Bräutigam and S. Miettinen (eds), Data Protection, Privacy and European Regulation in the Digital Age (Helsinki, 2016), Helsinki Legal Studies Research Paper 46, 2016. Available at SSRN: https://ssrn.com/abstract=2920181.

CHRISTAKIS, T.: Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR? In: Randal Milch and Sebastian Benthall (eds), "Cybersecurity and Privacy in a Globalized World – Building Common Approaches", New York University School of Law, 2019. Available at SSRN: https://ssrn.com/abstract=3397047.

CORRALES COMPAGNUCCI, M., ABOY, M. and MINSSEN, T.: Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs) (October 27, 2021). Available at SSRN: https://ssrn.com/abstract=3951085 and http://dx.doi.org/10.2139/ssrn.3951085.

DI PORTO F., GROTE T. and VOLPI, G.: Talking at Cross Purposes? A computational analysis of the debate on informational duties in the digital services and the digital markets acts. In Technology and Regulation, 2022, Special Issue: Should Data Drive Private Law, pp. 87-106. Available at https://techreg.org/article/view/11307/13774.

DRECHSLER, L. and KAMARA, I.: Essential Equivalence as a Benchmark for International Data Transfers After Schrems II. In: Kosta, Eleni and Leenes, Ronald, Research Handbook on EU data protection, Edward Elgar Publishing Ltd., 2021. Available at SSRN: https://ssrn.com/abstract=3881875 and http://dx.doi.org/10.2139/ssrn.3881875.

DRECHSLER, L.: What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights. In: Jusletter IT, Febr. 2019. Available at SSRN: https://ssrn.com/abstract=3549252.

GOICOVICI, J.: Clauzele privind drepturile consumatorilor în contractele de servicii cloud computing. In: Revista Română de Drept Privat, Nr. 2/2019, pp. 399-415.

GOICOVICI, J.: Consimțământul consumatorului la prelucrarea datelor personale în contractele business to consumer – condiția consimțământului granular. In: Analele Universității de Vest din Timișoara, Seria Drept, Nr. 2/2019, pp. 7-24.

GOICOVICI, J.: Portabilitatea datelor cu caracter personal, prin prisma dispozițiilor RGDP și ale Directivei 2019/770: este gambitul reginei mutarea de deschidere adecvată? In: Analele Științifice ale Universității Alexandru Ioan Cuza din Iași, Seria Științe Juridice, Tomul LXVII, Supliment 2, 2021, pp. 57-80.

GOICOVICI, J.: Dreptul relațiilor dintre profesioniști și consumatori. Bucharest: Hamangiu, 2022. 756 pages. ISBN 978-606-27-2024-7.

JAROVSCY, L.: Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs). In: European Data Protection Law Review, Vol. 4, Issue 4, 2018, pp. 447 – 458, DOI: https://doi.org/10.21552/edpl/2018/4/7.

JASMONTAITE, L., KAMARA, I., ZANFIR-FROTUNA, G. and LEUCCI, S.: Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. In: European Data Protection Law Review, Vol. 4, Issue 2, 2018, pp. 168 – 189, DOI: https://doi.org/10.21552/edpl/2018/2/7.

JURCYS, P., CORRALES COMPAGNUCCI, M. and FENWICK, M.: The future of international data transfers: managing legal risk with a 'user-held' data model. In: The Computer Law and Security Review, Vol. 46, 2022. Available at SSRN: https://ssrn.com/abstract=4010356 and http://dx.doi.org/10.2139/ssrn.4010356.
KAISER, E.: The Concept of 'Freely Given, Specific and Informed' Consent under the Scrutiny of the European Court of Justice. In: European Data Protection Law Review, Vol. 6, Issue 4, 2020, pp. 607-610, DOI: https://doi.org/10.21552/edpl/2020/4/19.
KE, T. and SUDHIR, K.: Privacy Rights and Data Security: GDPR and Personal Data Markets (July 5, 2020). Available at SSRN: https://ssrn.com/abstract=3643979 and http://dx.doi.org/10.2139/ssrn.3643979.
KUNER, Ch.: Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. In: University of Cambridge Faculty of Law Research Paper No. 20/2021. Available at SSRN: https://ssrn.com/abstract=3827850 and http://dx.doi.org/10.2139/ssrn.3827850.
LEISTNER, M.: The Existing European IP Rights System and the Data Economy – An Overview with Particular Focus on Data Access and Portability. In: Drexl J. (edt.), Data access, Consumer Protection and Public Welfare, Nomos, 2020, https://dx.doi.org/10.2139/ ssrn.3625712.
LEONARD P.: Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing in the Financial Services Sector (December 3, 2017). Available at https://ssrn.com/abstract=3154275.
LUNDQUIST, B.: An Access and Portability Right to Data – from a Competition Law Perspective. In: Faculty of Law, Stockholm University Research Paper No. 98, 2022. Available at https://ssrn.com/abstract=4022348 and http://dx.doi.org/10.2139/ssrn.4022348.
LUNDQUIST, B.: Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data. In: Bakhoum M., Conde Gallego B., Mackenrodt M.-O., Surblyté-Namavičienė G. (eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?, Springer, 2018, pp. 192-196.
LUZAK, J.: Digital age: time to say goodbye to traditional concepts. In: Journal of European Consumer and Market Law, Vol. 7, Issue 4, 2018.
MAHIEU, R.: The right of access to personal data: A genealogy. In: Technology and Regulation, 2021, pp. 62-75. Available at https://techreg.org/article/view/11001/11975.
RUBINSTEIN, I. and MARGUILIES, P.: Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground. In: Roger Williams University Legal Studies Paper 2021, Connecticut Law Review, 2021. Available at SSRN: https://ssrn.com/abstract=3786415 and http://dx.doi.org/10.2139/ssrn.3786415.
SWIRE, P. and KENNEDY-MAYO, D.: The Effects of Data Localization on Cybersecurity. In: Georgia Tech Scheller College of Business Research Paper No. 4030905, 2022. Available at SSRN: https://ssrn.com/abstract=4030905 and http://dx.doi.org/10.2139/ssrn.4030905.
SWIRE, P.: When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer. In: Georgia Tech Scheller College of Business Research Paper No. 3473187, 2019. Available at SSRN: https://ssrn.com/abstract=3473187 and http://dx.doi.org/10.2139/ssrn.3473187.
VOSS, W. G.: European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. In: Business Lawyer, Vol. 72, No. 1, 2017, pp. 221-233. Available at SSRN: https://ssrn.com/abstract=2894571.

Contact information:
Assist. Prof., Dr. Juanita Goicovici
E-mail: juanita.goicovici@law.ubbcluj.ro
University Babeș-Bolyai of Cluj-Napoca, Faculty of Law
Str. Avram Iancu, Nr. 11, Cluj-Napoca, Jud. Cluj
400089
Romania

POLITICIZATION THROUGH ALGORITHMS

Rastislav Funta

Danubius University, Janko Jesenský Faculty of Law

Abstrakt: V priebehu digitalizácie algoritmy čoraz viac preberajú funkcie formovania spoločenského poriadku. Koncepty ako algoritmická regulácia a riadenie algoritmov sa pokúšajú určiť funkciu algoritmov ako spoločenského poriadku. Skutočnosť, že čoraz viac sociálnych oblastí sa digitalizuje, a teda formuje pomocou algoritmov, priťahuje vo verejnej diskusii čoraz väčšiu pozornosť. Sociálne dôsledky tejto skutočnosti sú predmetom kontroverzných diskusií.

Abstract: In the course of digitalization, algorithms are increasingly taking on functions of social order formation. Concepts such as algorithmic regulation and algorithmic governance attempt to determine the social order function of algorithms. The fact that more and more social areas are being digitized and thus shaped by algorithms is attracting attention in the public debate. The social consequences of this are the subject of controversial debate.

1. INTRODUCTION

Algorithms are understood in the context of this article as computer-based methods of knowledge production that are characterized by a particular complexity. What is considered particularly complex varies depending on the context: Complexity can arise when processing data that is considered to be particularly large or novel. A particular complexity can also be inherent in the analysis process. The use of machine learning is considered to be a particularly complex form of knowledge generation in many areas. It is important that there is no cross-sectoral definition of when computer-aided processes count as algorithms. The term algorithm used here is defined more broadly than is usual in computer science, in order not only to designate narrowly defined artefacts, but also to include their social attributions.[1] The fact that more and more social areas are being digitized and are thus shaped by algorithms is attracting increasing attention in the public debate. There are technology-friendly interpretations that primarily see positive social effects, as they assume, for example, that social coordination through algorithms will become increasingly effective, efficient and inclusive. On the other hand, there are techno-skeptical interpretations that criticize algorithms for having a depoliticizing effect under the view of feigned objectivity, for obscuring power structures, and for entrenching social and political inequalities.[2] The politicization through algorithms primarily affects social norms; Algorithms only offer the opportunity to politicize them. Instead, politicization of algorithms aims directly at the algorithm, i.e. the way it is designed and in which context it is used. The central thesis of the article is that algorithms, unlike in blanket judgments, do not have a depoliticizing effect per se. Instead, the de-politicization of social norms by algorithms also leads to politicization processes by and through algorithms: social norms that were unchallenged are (again) called into question, and the concrete design of algorithms and their use is problematized.

2. ALGORITHMS AND DEPOLITICIZATION

In contrast to everyday language, in which depoliticization has negative connotations, it must be noted from a social science perspective that depoliticization is a necessary component of democratic societies.[3] Thus, democratic decisions are usually responses to design requirements that endure for a certain time, even if associated political conflicts are not resolved. Modem societies would

[1] FUNTA, R. (2019): Úvod do počítačového práva. MSD, Brno.
[2] ONDRIA, P. (2009): Basic Principles of Slovakia's Constitutionality. In. Współczesne państwo: wybrane problem, Wyższja Szkoła Bankowa, Poznaň.
[3] SITEK, M. (2022): Prawa człowieka. Pomiędzy ideologią a polityką. In. Polityka i Społeczeństwo.

be overwhelmed by the need to constantly politicize all social issues; the coordination effort would be immeasurable. Moreover, social structures require a certain stability in order to fulfill their (quite variable) purposes. Despite this, there are also critical interpretations in academic discourse that hold excessive depoliticization responsible for social inequalities and democratic decay. These narratives are followed by the social scientific discussion of algorithms, which sees them as ways for depoliticizing forms of order formation.

2.1. Algorithms and order formation

The fact that computer systems have a function of social order formation in numerous social areas is not a new topic of scientific debate. Rather, it goes back to the early days of the development of the first large computers and became virulent again and again in the various phases of the discourse. In the last ten years, the idea has been further developed and has produced concepts such as algorithmic governance, algorithmic regulation and algorithmic management. Compared to older concepts, they have a stronger social science foundation and also deal with the special features of computer programs. Although the concepts of algorithmic regulation and governance have different definitions and focuses, they have something in common: their subject matter are the processes and structures of social order formation that arise using computer-based calculation methods. The special features of algorithmic governance also include certain world views and norms that promote certain design claims and application practices. Thus, algorithmic governance is often characterized by strong future-oriented design claims and claims to act preventively ("preemptively") Further expectations associated with algorithmic governance are the higher objectivity, neutrality and validity of algorithmic calculations compared to calculations and evaluations performed by humans. As will be argued below, critical analyses see algorithms as an instrument that makes governance more technocratic.

2.2. Algorithms and technocratic governance

In the 1990s and early 2000s, the internet[4] and digital technologies were seen as enabling factors for social inclusion and political participation. But while these promises have not faded, studies of the participatory potential of digital technologies indicate that many of those hopes have been dashed. In contrast to the promise of participation, we identify digital technologies as a central pillar of technocratic governance, the form of government that has been dominant for the past decades. Here, digital technologies are elements of a form of cybernetically inspired governance that relies on expertise and representation with little responsiveness. Numerous socio-theoretical interpretations of digitization describe the characteristics of the connection between digitization, technocratic rule and depoliticization. The technocratic character of digitally supported rule is also based on the fact that transnational technology companies are less and less socially embedded and are (still) little politically controlled.

Although the concepts of algorithmic regulation and governance have different definitions and emphases, they have common features: Their subject matter is the processes and structures of social order formation that emerge using computer-based computational methods.[5] They also emphasize certain technical aspects of algorithmic knowledge production: these include the structuring of social reality with the help of mathematical models that are often based on probability theories; a focus on pattern recognition; risk analyses; inference calculations; and machine learning. The special features of algorithmic governance also include certain world views and norms that promote certain design claims and application practices. For example, algorithmic governance is often characterized by strong future-oriented design claims and claims to act preventively. Other expectations associated with algorithmic governance include the higher objectivity, neutrality, and validity of algorithmic computations compared to computations and evaluations performed by humans. As will be argued

[4] ŠRAMEL, B. - HORVÁTH, P. (2021): Internet as the communication medium of the 21st century: do we need a special legal regulation of freedom of expression on the internet? In. The Lawyer Quarterly. No. 1.
[5] GREGUŠOVÁ, D. - DULAK, A. - CHLIPALA, M. - SUSKO, B. (2005): Právo informačných a komunikačných technológií. Vydavateľské oddelenie STU, Bratislava.

below, critical analyses accordingly see algorithms as an instrument that makes governance more technocratic.

3. ALGORITHMS AND POLITICIZATION

If one wants to understand the relationship between algorithms and politicization, one cannot consider algorithms holistically, i. e. as artefacts standing in their own right. Nor can they be understood as tools or autonomous agents: Machines are not just human tools, and humans are not the executors of machine decisions.[6] Corresponding readings lead to generalized judgments of algorithms as instruments of depoliticization (or more rarely: of resistance). For a differentiated analysis, on the other hand, a technical-scientific approach is helpful, which understands algorithms more as elements in complex socio-technical systems that are composed of human and machine agents and that exhibit numerous entanglements. algorithms are understood by me in the following as a technical formalization and quantification of procedural rules from which social norms or organizational norms can be read. This approach draws attention to the numerous components of algorithmic procedures and practices, such as the database, the calculation methods, the interpretation of information, the transparency of the entire system, etc. From this perspective, controversies about algorithms can be understood as the politicization of social norms.

3.1. Politicization of algorithms in the realm of state rule

The COMPAS score, described below, can be used to examine how algorithms are used to de-politicize and re-politicize complex and sensitive decisions. Central norms negotiated here were racial discrimination and poverty in the context of equality before the law.[7]

One case of algorithmic regulation in the sphere of state control, on which much research is already available, is the use of algorithms in the administration of justice, as is common in the USA. In concrete terms, individual risks of recidivism of defendants are calculated and aggregated into risk scores, which are available to judges in their sentencing decisions. Although there are differing findings on the extent to which judges base their judgments on scores, the score itself already signifies a contingency closure of the complex assessment of the social risk emanating from an accused person. The specific procedures vary by state and there are different software. Two widespread ones are the LSI (level of service inventory) and the COMPAS score. The latter gave rise to a major public controversy due to the fact that the score racially discriminates by generating different error rates for white and black accused, to the detriment of the latter. The corresponding media and scientific controversy concerned numerous aspects of the algorithmic system: On the one hand, the mainstream media discussed in detail for the first time that algorithms cannot keep the promise of objectivity as long as they operate on data sets that show social inequalities and in which delinquency is unequally distributed by race. An important finding about algorithmic systems was that it is not enough to exclude information from data sets that is obviously relevant to discrimination. Because other information that does not appear relevant to discrimination at first glance, such as place of residence, professional career or criminal history, can appear as indicators (proxies) for sensitive information such as gender and ethnic background and lead to discriminatory results. The fact that supposedly neutral risk scores can correct the subjective and possibly racially discriminatory attitudes of judges has since been up for discussion. In a second step, however, further aspects of the use of algorithmic scores in case law were problematized, such as the expansion to more and more application contexts. This has been criticized as a misappropriation that is not valid and perpetuates social inequalities. This conflict regarding the general expansion of deposit payments does not only exist in connection with algorithmically generated risk scores, but has been reconsidered on the basis of them. Moreover, it has been questioned whether risk scores, as intended, actually reduce

[6] YARA, O. – BRAZHEYEV, A. – GOLOVKO, L. - BASHKATOVA, A. (2021): Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects. In. European Journal of Sustainable Development. Tom. 10.

[7] SITEK, B. (2013): The human right to respect the religious identity in the light of the media and political regulation. In. Sitek, M., Dammacco, G., Ukleja, A., Wójcicka, M. (eds) Europe of Founding Fathers: Investment in the common future. Olsztyn.

incarceration rates by increasing judges' imposition of resocialization measures. So far, this promise of algorithmic risk calculations does not seem to be fulfilled either. Finally, the politicization of the COMPAS score has led to a fundamental debate about the rationalities of adjudication and how to balance different goals, such as sanction and resocialization or individual versus group fairness.

Another area in which algorithms are frequently used is the evaluation of recipients of social benefits. The goal is usually to allocate benefits more effectively, efficiently and/or fairly, as well as to combat fraud. One example that sparked a controversy is gender discrimination[8] in the labor market and the orientation of the solidarity principle via the so-called AMS algorithm. This refers to the software-based assessment of the labor market chances of the unemployed by the Austrian Public Employment Service (AMS). At the center of the controversy was the question of whether the allocation of social benefits should follow a logic of cost efficiency, as pursued by the AMS algorithm, or whether it should be subject to a logic of need. In the debate, this boiled down to the question of whether, given limited subsidies, populations that are particularly close to the labor market or rather far from it should be subsidized. This is because the software divides unemployed individuals into three groups according to their predicted chances of reintegrating into the labor market: high, medium and low chances. The medium group will receive the most funding resources. The AMS's argument is that members of the group with high integration chances could find a job on their own and that those with low chances are hardly employable.

Another controversy concerned possible discrimination against women. The characteristics gender, age group, education, health impairment, care obligations and occupational group are included in the calculation of the probability of integration.[9] In contrast to the case of the COMPAS score, in which ethnic characteristics are not explicitly included in the data set but rather appear latently, the characteristic gender is explicitly included in the calculation. Since female gender contributes to a poorer integration score, the AMS algorithm has been criticized as discriminatory. The AMS defended itself against this accusation with the reference that it was not the algorithm that was sexist, but the labor market. Since the model was developed using data on labor market integration over the past years, it merely reflects existing social inequalities without normatively supporting them.

3.2. Politicization of algorithms in the private sector

Two areas of application of algorithmic regulation in the private sector that are causing particularly great controversy are the algorithmic management of female employees and the algorithmic credit assessment of consumers.

Companies are increasingly using software to evaluate their employees. One example is the fashion retailer Zalando, which uses the Zonar system to evaluate the performance of its employees and, on this basis, to make decisions about their career development and remuneration. This has led to de- and re-politicization with a view to corporate co-determination and fair wages. A central element of the software is the extraction and combination of horizontal evaluation of data (worker-coworker ratings) and their automated processing into individual scores. From the management's point of view, the evaluation of employees is now fairer than it used to be, since it is no longer carried out by immediate supervisors alone, but includes more perspectives, such as those of colleagues, customers and managers, and is based on a broader set of indicators.

Another social context in which algorithms have played an important role for many years is the evaluation of consumers using so-called credit ratings and the implications for their access to markets. In the U.S., where credit scores even determine access to health insurance, unemployment insurance, and pension plans, there is also increasing criticism of the lack of transparency and control of scores, and the suspicion that they reinforce social inequalities. A score that predicts the likelihood of repaying a loan installment on time cannot be readily reinterpreted as the likelihood of paying bills or rent. A

[8] SVÁK, J. (2000): Zásady a tendencie v ochrane práva na súkromie. In. Justičná revue, č. 11.
[9] HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol. (2018): Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov – Veľký komentár. Eurokódex, Bratislava.

de-politicization of social norms through the use of algorithms (depoliticization through algorithms) is understood as the closing of contingency spaces through a formalization of decisions in the form of algorithms or software. Specifically, this applies to decisions regarding the risk assessment, the assessment of the chances of unemployed persons to get job, the performance assessment of employees and the creditworthiness of consumers.[10]

4. PECULIARITIES OF THE POLITICIZATION OF ALGORITHMS

This chapter wants to describe, why algorithms offer themselves as a reason for the politicization of social norms and structures. The expansion of digital processes into more and more social spheres means that the contexts in which people come into contact with the functions of algorithms that are perceived as pleasant or irritating, for example in the context of welcome or counterintuitive consumption recommendations, are multiplying. However, advancing digitization alone can hardly explain the politicization potential of algorithms. Thus, one can assume that technical properties of algorithms are one reason for their politicization.

Certain aspects of algorithms played a role in all conflicts, namely their inherent formalization, quantification and objectification of complex social phenomena and norms. Algorithms operate on the basis of a variety of definitions regarding the database, data preparation, calculation and interpretation. Algorithms require numerous operationalizations of norms, rules, goals, standards and sub-standards. These, in turn, must all be placed in a clear relationship to each other so that calculations are possible. Algorithms codify social issues that can actually be shaped politically and perpetuate them. Nevertheless, formalization and quantification can challenge politicization. Because only the formalization of social norms makes them accessible for criticism and design. This happens, for example, when the decision-making premises of machines are problematized, as is typical for the debate of biased datasets, or when the validity or legitimacy of computational procedures for a particular application purpose is questioned.

Another aspect of algorithms is increasing doubts about the intelligibility of machine processes. In principle, machines were previously considered to have a comparatively high degree of comprehensibility and intelligibility compared to human decisions; machines were considered to be understandable and coherent in principle because they consistently make decisions according to programmed rules. Through unsupervised machine learning, there are now machines that themselves define and change the rules of decision-making - in part in ways that cannot be reconstructed and explained either by developers or by the machine itself. This novel opacity of computers fuels public distrust of machine-made decisions. Although the partial opacity of algorithms has long been a topic of discussion in computer science, it is only in the last years that the issue has received significant critical attention in public opinion. One consequence of the distrust of algorithms and their possible social risks is to make them available for inspection and analysis by the public, researchers and/or an independent supervisory authority. As an expression of society's demand to understand and scrutinize algorithms, numerous practices have emerged, such as blackbox testing, and reverse engineering. These are procedures that attempt to reconstruct the functioning and effect of algorithms.

5. CONCLUSION

This article has examined the relationship between algorithms and de- or (re-)politicization. Cases in which algorithms have been strongly politicized in recent years have shown that disputes about algorithms have called into question both the material order in societies and the reflexive order. For example, the formalization of decision rules and social norms in algorithms has prompted the questioning of important norms in the administration of justice, the allocation of social benefits, and the evaluation of employees and consumers. Controversial evaluation and decision rationales were, for example, an orientation towards risks, the primacy of cost efficiency, horizontal evaluation in companies. In the cases studied, politicization through algorithms was thus always linked to larger

[10] MISKOLCZI-BODNÁR, P. (2020): A fogyasztók tájékoztatása és a digitalizáció [Consumer information and digitization]. In. Homicskó, Árpád Olivér (ed.) The effect of digitization in certain areas of law, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, Budapest.

social conflicts, which were, however, difficult to grasp.This article supplements the narrative that algorithms generally have a depoliticizing effect with the realization that algorithms can certainly have a politicizing effect and have numerous properties that lend themselves very well to politicization. This is important for public discourse, since the possibilities for designing algorithms and regulating transnational technology groups and state authorities with a view to algorithmic processes have only just been spelled out. A look at the politicization of algorithms shows that in this context not only social inequality and individual rights violations are denounced, but also the (meta)structures of the protection of individual rights and social norms are negotiated. Against this background, the argument that social and political participation and control are out of reach due to a lack of ideas appears highly motivated.

Literature summary:

FUNTA, R. (2019): Úvod do počítačového práva. MSD, Brno.
GREGUŠOVÁ, D. - DULAK, A. - CHLIPALA, M. - SUSKO, B. (2005): Právo informačných a komunikačných technológií. Vydavateľské oddelenie STU, Bratislava.
HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol. (2018): Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov – Veľký komentár. Eurokódex, Bratislava.
MISKOLCZI-BODNÁR, P. (2020): A fogyasztók tájékoztatása és a digitalizáció [Consumer information and digitization]. In. Homicskó, Árpád Olivér (ed.) The effect of digitization in certain areas of law, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, Budapest.
ONDRIA, P. (2009): Basic Principles of Slovakia's Constitutionality. In. Współczesne państwo: wybrane problem, Wyższja Szkoła Bankowa, Poznaň.
SITEK, M. (2022): Prawa człowieka. Pomiędzy ideologią a polityką. In. Polityka i Społeczeństwo. 20.01:145-159.
SITEK, B. (2013): The human right to respect the religious identity in the light of the media and political regulation. In. Sitek, M., Dammacco, G., Ukleja, A., Wójcicka, M. (eds) Europe of Founding Fathers: Investment in the common future. Olsztyn.
SVÁK, J. (2000): Zásady a tendencie v ochrane práva na súkromie. In. Justičná revue, č. 11.
ŠRAMEL, B. - HORVÁTH, P. (2021): Internet as the communication medium of the 21st century: do we need a special legal regulation of freedom of expression on the internet? In. The Lawyer Quarterly. No. 1.
YARA, O. – BRAZHEYEV, A. – GOLOVKO, L. - BASHKATOVA, A. (2021): Legal Regulation of the Use of Artificial Intelligence: Problems and Development Prospects. In. European Journal of Sustainable Development. Tom. 10.

Contact details:

Dr. habil. JUDr. Rastislav Funta, Ph.D., LL.M.
Vice-Rector
Danubius University
Richterova 1171
925 21 Sládkovičovo
rastislav.funta@vsdanubius.sk

DOCTOR - ROBOT OR AUTOMATED PROVISION OF HEALTHCARE - IS IT LEGALLY POSSIBLE?

Soňa Sopúchová

Comenius University in Bratislava, Faculty of Law

Abstract: Information and communication technologies find their application in most areas of life, and their influence and use become the subject of many legal questions, challenges, and discussions. The information society goes hand in hand with automation, which started already in the last century with the use of human-controlled machine technology. Nowadays, automation has moved even further, with regard to machines operating on the principles of artificial intelligence. These changes also affect the health sector. Therefore, in the article, the author analyzes how elements of automation can be used in connection with artificial intelligence in the provision of health care. In the introduction, the author presents the basic theses and principles of health care provision with an emphasis on the electronisation of processes falling under the issue of e-Health. The core of the article focuses on the question of which entities are legally authorized to provide health care and whether a machine working on the principle of artificial intelligence, the so-called robot, can be included among these entities. The goal of the analysis is to assess whether in the Slovak legal environment and practice it is possible to consider a doctor - robot and, if so, within what limits. The article provides answers to the basic questions of automation in the provision of health care, draws attention to existing legal challenges, and highlights other emerging issues.

Abstrakt: Informačno-komunikačné technológie náchadzajú svoje uplatnenie vo väčšine oblastí života a ich vplyv a využívanie sa stáva predmetom mnohých právnych otázok, výziev a diskusií. Informačná spoločnosť ide ruka v ruke s automatizáciou, ktorá začala už v minulom storočí využívaním strojovej techniky ovládanej človekom. V súčasnej dobe sa automatizácia posunula ešte ďalej, a to vzhľadom na stroje fungujúce na princípe umelej inteligencie. Tieto zmeny sa dotýkajú aj sféry zdravotníctva. Autorka preto v príspevku analyzuje, akým spôsobom možno využívať prvky automatizácie v spojistosti s umelou inteligenciou pri poskytovaní zdravotnej starostlivosti. Autorka v úvode uvádza základné tézy a zásady poskytovania zdravotnej starostlivosti s akcentom na elektronizáciu procesov spadajúcu do problematiky e-Health. Jadro príspevku sa sústredí na otázku, ktoré subjekty sú opravnené zákonným spôsobom poskytovať zdravotnú starostlivosť a či medzi tieto subjekty možno zaradiť aj stroj pracujúci na princípe umelej inteligencie, tzv. robot. Cieľom analýzy je posúdenie, či v slovenskom právnom prostredí a praxi možno uvažovať o lekárovi – robotovi a ak áno, v akých medziach. Príspevok prináša odpovede na základné otázky automatizácie pri poskytovaní zdravotnej starostlivosti, upozorňuje na existujúce právne výzvy a zdôrazňuje ďalšie vznikajúce otázky.

Keywords: automation in healthcare, e-Health, artificial intelligence in healthcare, doctor – robot

Kľúčové slová: automatizácia v zdravotníctve, e-Health, umelá inteligencia v zdravotníctve, lekár – robot

1 INTRODUCTION

A number of technological changes, a great dynamic of development characterize the current society and a different way of processing information than it was in the past. In several cases today, we work with information, communication and other means, which by their activity affect the rights of individuals and for that reason must be legally regulated. Today, modern technologies greatly influence, for example, the processing of personal data, delivery, whether on a private level or on the level of official communication with state authorities, the investigation of illegal or unauthorized actions, and provide many other possibilities. It has only been a few decades since the legal systems

of individual states had to deal with the arrival of personal computers, mobile phones, later with intelligent devices such as smartphones or tablets, or with the expansion of the Internet and social networks. Their use affected several legal areas and resulted in the emergence of important legal questions and challenges. The European Union has gradually adopted strategic documents and normative legal acts, which have newly modified the topics of the aforementioned personal data, copyright or electronization of several legal areas, for example, public administration (e-government), judiciary (e-justice), or health (e-health). During this period, the field of robotics and computer programs also developed in parallel, and in recent years, this has developed to the extent that even experts from the field of law have begun to deal with it. The reason is the fact that technological development has reached a stage that must be clearly reflected in the legal systems of states. More specifically, we are talking about technologies that have the prerequisites to intervene in various areas of social life, with serious consequences, whether human, ethical, or legal. As a follow-up to the above, in the article we will discuss the existence and operation of artificial intelligence, which is capable, together with other technologies, for example, of providing transport in the form of so-called autonomous cars, diagnose diseases and recommend adequate treatment, perform surgical operations, assess the factual and legal situation and make decisions based on that, create contracts and other legal documents, filter the wrong candidates for employment or replace human limbs with artificially intelligent prosthetic devices.

The aim of this article is to carry out a legal analysis of the question of whether a machine can provide health care, and therefore whether in this case we can talk about the automation of health care. In connection with this, a sub-question arises whether it will be exclusively a machine controlled by a human or it can also be a machine working based on artificial intelligence. The first part of the article includes clarification of the provision of health care, including an analysis of who can be a health care provider. In the second part, we discuss the concept of artificial intelligence, we provide a brief historical view of its origin, and the possibilities of its use in society, pointing out possible risks. In the end, we will try to answer the above question and summarize the findings that can help in further discussion.

2 PROVISION OF HEALTH CARE IN THE SLOVAK REPUBLIC DE LEGE LATA

Health care has its legal definition in 2 par. 1 of Act no. 576/2004 Coll. on health care, services related to the provision of health care and on the amendment of certain laws (hereafter also "Act on Health Care"), where it is defined as "*a set of work activities performed by health workers, including the provision of medicines, medical aids and dietetic foods with the aim of prolonging the life of a physical person, increasing the quality of his life and the healthy development of future generations; health care includes prevention, dispensary, diagnosis, treatment, biomedical research, nursing care and midwifery*."[1] The right to health care is guaranteed in international conventions to which the Slovak Republic is a signatory, namely the Universal Declaration of Human Rights[2], the International Covenant on Economic, Social, and Cultural Rights[3] and the Convention on Human Rights and

[1]Article 2 par. 1 of the Act on Health Care.

[2]Article 25 par. 1 of the Universal Declaration of Human Rights: "*Everyone has the right to a standard of living that ensures his and his family's health and well-being, including food, clothing, housing, medical care and necessary social measures; he has the right to security in the event of unemployment, illness, incapacity for work, widowhood, old age or in other cases of loss of earning potential caused by circumstances beyond his control.*"

[3]Article 12 par. 2 of the International Covenant on Economic, Social, and Cultural Rights: "*States, parties to the covenant, will take measures to achieve the full realization of this right, which will include: a) measures to reduce the number of abortions and infant mortality and measures for the healthy development of the child; b) improvement of all sites external living conditions and industrial hygiene; c) prevention, treatment and control of epidemic, local diseases, occupational diseases and other diseases; d) creation of conditions that would provide everyone with medical assistance and care in case of illness*."

Biomedicine.[4] Following these documents, the right to health care was enshrined in Act no. 460/1992 Coll. The Constitution of the Slovak Republic (hereafter also the "Constitution of the Slovak Republic"), among economic, social and cultural rights.[5] The Slovak Republic fulfills its positive commitment to ensure the realization of the right to health care for its citizens through the national health policy and the health care provision system.

According to the current Slovak legislation, health care and services related to it can be provided exclusively **by healthcare providers** and **healthcare professionals** under the conditions established by a special regulation, which is Act no. 578/2004 Coll. on health care providers, health professionals, and state organizations in the health sector and on the amendment of certain laws as amended by later legislation (hereafter also the "Law on Providers"). These entities providing health care are obliged to provide health care *correctly.* This means that healthcare professionals should perform all medical procedures to correctly determine the disease with the provision of timely and effective treatment with the aim of healing the patient or improving his condition, taking into account the current knowledge of medical science and in accordance with standard procedures for performing prevention, standard diagnostic procedures, and standard therapeutic procedures taking into account the individual condition of the patient.[6]

In the Slovak Republic, health care is provided in **several forms**, such as **ambulatory care, institutional care, pharmacy care and nursing care in social assistance facilities**.[7] In addition to the mentioned forms of health care provision, the Health Care Act regulates services related to the provision of health care, which are the provision of meals during the provision of institutional care; provision of bed rest during the provision of institutional care; processing of data obtained during the provision of health care in electronic form for the purposes of health insurance; statistical processing of medical prescriptions for health insurance purposes and more.

2.1 Entities providing health care

When analyzing entities that can operate in the processes of providing health care, we are based on the Act on Providers. This recognizes **healthcare providers and healthcare professionals.** Even before we clarify these concepts in more detail, we state that the Act on Providers establishes a condition for the provision of health care, which is the fulfillment of the conditions for the performance of the medical profession, which is another concept that needs to be worked with.

The healthcare provider can be:

a) a natural person-entrepreneur or legal entity that provides health care on the basis of a permit or a license for the provision of pharmaceutical care according to a special regulation; trade license according to a special regulation or on the basis of a decision on the regulation of the creation of a mobile collection point,
b) a natural person-entrepreneur who provides health care on the basis of a license for independent medical practice,
c) a natural person-entrepreneur or legal entity that provides health care on the basis of a permit to operate a natural healing spa or a permit to operate a spa clinic according to a special regulation,
d) a natural person, based on the approval of the Ministry of Health of the Slovak Republic for the temporary and occasional exercise of the medical profession.[8]

[4]Article 3 of the Convention on Human Rights and Biomedicine: "*Contracting parties shall take appropriate measures within their jurisdiction to ensure equitable access to health care, taking into account both the need for health care and available resources."*
[5]Article 40 of the Constitution of the Slovak Republic: "*Everyone has the right to health protection." On the basis of health insurance, citizens have the right to free health care and medical aids under the conditions established by law*."
[6]Article 4 par. 3 of the Act on Health Care.
[7]Article 7 par. 1 of the Act on Health Care.
[8]Article 4 of the Act on Providers.

In the sense of the above, it is true that the healthcare provider is not always an entity that would perform a health profession, it is an administrative umbrella for the provision of health care, within which it is provided by healthcare professionals. However, it is also true that a healthcare professional can act as a healthcare provider.

The healthcare professional is regulated in the next part of the Act on Providers, specifically in the provision of § 27 on the performance of the healthcare profession. The law stipulates that a healthcare professional is a **natural person** who **performs some of the listed health professions** (e.g. doctor, dentist, pharmacist, nurse, masseur or orderly). The legislator also defines the **conditions for the performance of the medical profession**, which are:

1. *full capacity for legal acts,*
2. *medical capacity, professional capacity,*
3. *integrity,*
4. *registration,*
5. *credibility, which is only required in some cases*.[9]

Regarding the question of which entity can provide health care, after careful consideration, we arrive at the opinion that everyone who performs a health care profession provides some form of health care. This means that the first condition for the possibility of providing health care is that it must be a healthcare professional. The difference between a healthcare provider and a healthcare professional is that a healthcare professional is always a specific natural person with a medical education practicing a health profession, while a provider can also be a legal entity (commercial company, nonprofit organization, budget organization, etc.) that holds a license or permit to provide health care. This initiative is also important from the point of view of our further considerations on the automated provision of health care. In this case, the Slovak legislator stipulates that the **health profession is a set of work activities** performed by a healthcare professional in:

a) provision of health care,
b) provision of emergency medical services,
c) to protect people's health,
d) medical assessment activity,
e) handling medicines and medical devices,
f) performing control of the provision of health care, protecting people's health and medical assessment activities and performing supervision of health care,
g) provision of care to people in detention.[10]

At the end of this section, we summarize that the provision of health care is one of a set of work activities that a healthcare professional within a specific health profession. Due to legal conditions, only a **natural person can be this person**.[11] However, automation in conjunction with artificial intelligence is already being used in this area as well and theoretically "breaks" customary standards, because in January 2022 the first operation performed by an autonomous robot without human intervention took place in the USA. It was a laparoscopic surgery on the soft tissue of pigs (specifically, the connection of the two ends of the intestinal tract[12]), which was performed at the university level. We will talk more about this case and other contexts in the third chapter of this article.

3 AUTOMATION AND ARTIFICIAL INTELLIGENCE IN HEALTHCARE

Until recently, artificial intelligence was only known to society from the film industry or science fiction literature. Currently, this is one of the most discussed topics in marginal legal areas dedicated to the connection of law and technology, but it is increasingly being mentioned in debates about traditional legal institutes, because its use affects the areas of legal responsibility, criminal

[9]Article 31 par. 1 and 2 of the Act on Providers.
[10]Article 3 par. 1 of the Act on Providers.
[11]Article 27 par. 1 of the Act on Providers.
[12]This is one of the most demanding operations of the digestive tract, because the surgeon must be precise and thorough, considering that even the smallest mistake can lead to leakage, which can have life-threatening consequences for the patient.

proceedings or copyright. We do not find a legal definition of the term artificial intelligence in any legal order. Since the sixties of the last century, however, we have found a number of professional definitions and clarifications, based on which we can work with this term for the purposes of variously defined goals.

As we have already mentioned several times, artificial intelligence also finds application in the field of healthcare. This technology can be applied in various aspects of healthcare, such as providing a system to analyze medical information to determine the sources of errors and develop solutions using existing results and adding computer intelligence to medical devices and tools. Remote monitoring of a patient's health and treatment or devices that can perform an operation or surgery can also be considered elements of artificial intelligence in the healthcare sector. Other examples of the use of artificial intelligence in healthcare are as follows:

- *the use of algorithms in disease diagnosis,*
- *the use of virtual reality during surgical procedures,*
- *applications in the form of chat boxes, online platforms or discussion forums,*
- *the use of robotic devices in the care of patients in hospitals,*
- *fully automatic robots, so-called "digital doctors"*.[13]

3.1 Automation in the provision of health care

The term automation is based on several levels, and in general, it can be understood as a wide range of technologies that reduce human intervention in processes, however does not completely exclude human participation. Automation still leaves the control and management of the work of machines to people, although with the continuous development of artificial intelligence, machines are increasingly taking over these functions as well. For the purposes of this article, we decided to focus mainly on the field of robotic operations, because it is in this field that elements of automation and artificial intelligence can be observed to the greatest extent.

The discussion about the possibility of providing health care through machines naturally moves into the sphere of robotic operations. These are remote operations carried out with the help of robots. Robotic operations are included in telemedicine, the so-called distance medicine, which is part of e-Health. The European Commission emphasizes in its materials that telemedicine includes a wide range of services. The most frequently mentioned are teleradiology, telepathology, teledermatology, teleconsultation, telemonitoring, telesurgery, and teleophthalmology. Other services include call centers and online patient information centers, remote consultations, electronic home visits or video conferencing.[14]

The history of robotic operations dates back to the early 1980s. The first surgical robot, called Arthrobot, was developed in 1983 and was first used in Vancouver, Canada. We can also mention the Zeus robot or the da Vinci robot. The latter is considered a leader in this field. In robotic operations, the surgeon controls the robot remotely, within the same room or even transcontinentally, which is why in theory and practice we can also encounter the term telerobotics or telesurgery. In this case, the expression robot-assisted surgery is more accurate, because the operation is performed by the surgeon and the robot "only" transmits his movements, while removing deviations (for example, in the path of the surgeon's hand), ensuring greater accuracy and control of the operation above the level of the human factor.[15] However, the use of artificial intelligence is under great development. For example, robots can prevent a surgeon from moving if they think they might be dangerous. In such a situation, they require the surgeon to confirm the movement and then proceed with the operation. Here we come to the question of technological security, because it is not excluded that the robot will not request confirmation, or even after confirmation, the operation will not continue. An example is the

[13]GOMEZ-GONZÁLES, Emilio – GOMEZ-GUTIERREZ, Emilia. *Artificial Intelligence in Medicine and Healthcare: applications, availability and societal impact* . Luxembourg: Publications Office of the European Union, 2020, p. 27.
[14]EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society* . 2008, p. 3.
[15]WEDNESDAY, Leoš – HÁNA, Karel. *eHealth and telemedicine* . Prague: Grada Publishing, 2016, p. 79.

case of robotically assisted surgical devices (RASDs), which surgeons use to operate small cutting tools instead of using ordinary scalpels. If a surgeon's hand slips with a scalpel and a vital tendon is cut, the intuitive feeling is that the surgeon is the primary responsible for the error. But what if the surgeon uses the RASD system, which is marketed as a special "tendon avoidance program", similar to the alarms in cars when their sensors signal an imminent collision? If the tendon sensors fail and the error warning does not sound, can the injured patient sue the RASD vendor? Or just a doctor who relied on it?[16] These are just the initial questions we can ask ourselves during this discussion. Another related question is why should even we deal with the use of artificial intelligence in the provision of health care at various levels, including the legal one?

Analysis prepared for the European Parliament's Committee on the Environment, Public Health, and Food Safety entitled ***Robots in Healthcare: Solution or problem?*** states that the health sector within the European Union faces growing demands for services brought about by the aging of the population, the increase in chronic diseases, budget restrictions, and the lack of qualified healthcare professionals. According to the authors of this analysis, technological developments in the field of robotics and artificial intelligence can provide countless opportunities to solve these challenges, which would lead to significant cost savings. Along with the integration of digital technologies, the application of robotics and artificial intelligence could lead to improvements in medical diagnosis, surgery, disease prevention and treatment, and support for rehabilitation and long-term care. Some of the most interesting applications for the health care sectors, according to the analysis, include:

- **robotic surgery** enabling more precise, less invasive and remote interventions that rely on the availability and evaluation of data;
- **nursing and social assistance robots** enabling to meet the growing demands for long-term care of the aging population affected by multimorbidity;
- **rehabilitation systems** supporting the recovery of patients, as well as their long-term treatment at home and not in a medical facility;
- **training for health care professionals** offering support for continuous training and lifelong learning initiatives.[17]

On the one hand, the integration of digital technologies, robotics, and artificial intelligence promises revolutionary changes in the healthcare sector, but on the other hand, we cannot ignore several important ethical, legal, socio-economic, and technological challenges that must be addressed in order to unlock the potential of these technologies.[18] The legal aspects must be the subject of extensive discussion even before the introduction of autonomous robots into the processes of providing healthcare. **Legislation** and **especially issues of legal responsibility** can be identified as problematic points.

Given that artificial intelligence and digitization are based on the collection and access to a large amount of data, including personal data, in some cases it can also involve the analysis of sensitive data, issues of privacy, processing and sharing of personal data or their security arise. If we focus on the field of health care provision, we naturally come to institutions such as informed consent, health documentation, data ownership, all in light of the European regulation of personal data protection (GDPR). It is precisely the categories of privacy and personal data that tend to create problematic points in the healthcare industry for the coexistence of artificial intelligence, digitalization,

[16]PASQUALE, Frank. *When medical robots fail: Malpractice principles for an era of automation.* In: Teach Stream. Available at: https://www.brookings.edu/techstream/when-medical-robots-fail-malpractice-principles-for-an-era-of-automation/

[17]DOLIC, Zrinjka – CASTRO, Rosa – MOARCAS, Andrei. *Robots in healthcare: a solution or a problem?* , Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 7.

[18]DOLIC, Zrinjka – CASTRO, Rosa – MOARCAS, Andrei. *Robots in healthcare: a solution or a problem?* , Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 7.

robots, and the protection of these areas. In this context, we draw attention to the opinion of the author Pierce from the University of Tilburg, who stated that the issues of privacy and data protection fall into two dimensions: *regulatory* and *principled.* The regulatory dimension concerns the General Data Protection Regulation (GDPR). She stops there and expresses the opinion that this regulation is limited on the subject of the use of robots in medical and clinical facilities. As an example, she gives the definition of the principle of data minimization, which requires that the processing of data should be relevant and limited to the purposes for which it is collected. This is problematic, according to Pierce, because all types of information collected for this purpose (eg, behavioral changes, speech patterns, geospatial monitoring, etc.) can be interpreted as relevant to health status. Another important aspect she mentioned is the complexity of consent requirements that need to be defined in relation to data processing, care and intervention.[19] Another example is the reference to Article 22 of the GDPR on automated decision-making, which states that a person has the right to an explanation of how decisions concerning him have been made. As author Pierce points out, it is highly unlikely that a robot could provide this information and if so, it would pose a problem for the legally required doctor-patient relationship.[20] We agree with the above and add that the regulation on personal data protection and its importance are indisputable, but we believe that it was prepared for certain segments of personal data processing and it will be increasingly difficult to apply it across the board in all areas of society.

3.2 Legal responsibility of the robot

Robots are currently used in the provision of healthcare mainly as tools for a surgeon or other doctor. These are, for example, robotic arms that are capable of various long-term activities that cause fatigue or overload in the case of a person; they can also be the delivery of other instruments or laparoscopic instruments. However, the biggest revolution was caused by the incorporation of artificial intelligence, and thus the use of machine learning. Namely, if it happens that the robot is capable of evaluating a case or situation with the subsequent creation of a decision that tends to cause certain consequences in the outside world, it is necessary to think about the responsibility side. This means being prepared to answer the question of who will be held responsible in the event of an error, as it has been established that even robots make mistakes.[21] As we mentioned in the second chapter of this article, at the beginning of 2022 a unique surgical procedure took place, when the STAR robot (Smart Tissue Autonomous Robot) performed laparoscopic surgery on the soft tissue of a pig without the guiding hand of a human, which is considered in the scientific world to be a significant step towards fully automated surgery on humans. The Smart Tissue Autonomous Robot or STAR was designed and put into operation by a team of researchers from Johns Hopkins University located in the United States of America.

Despite the fact that technological companies are making progress in developing autonomous devices ensuring the full functioning of various activities and functionalities at high speed, their real use is not yet possible in many cases. Just as in the case of autonomous vehicles, also in the case of the use of elements of artificial intelligence or autonomous robots in the healthcare sector, one of the most pressing questions is precisely the question of legal responsibility.

If we look at it in the context of the legal environment of the Slovak Republic, the basic and general legal regulation of liability for damage is found in Act no. 40/1964 Coll. Civil Code (hereafter

[19]DOLIC, Zrinjka – CASTRO, Rosa – MOARCAS, Andrei. *Robots in healthcare: a solution or a problem?* , Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 16.

[20] DOLIC, Zrinjka – CASTRO, Rosa – MOARCAS, Andrei. *Robots in healthcare: a solution or a problem?* , Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 19.

[21]PASQUALE, Frank. *When medical robots fail: Malpractice principles for an era of automation.* In: Teach Stream. Available at: https://www.brookings.edu/techstream/when-medical-robots-fail-malpractice-principles-for-an-era-of-automation/

also "Civil Code"), namely in Section 415: " *Everyone is obliged to act in such a way that there is no damage to health, property, nature, and the environment*."[22]

An integral part of the provision of health care is the risk that the doctor will make a mistake while providing it. Doubts can be of the nature of a one-time manual failure (for example, the skill of the operator), but they can also be the result of an incorrect diagnostic or therapeutic procedure. Such misconduct can (but does not necessarily) harm the patient's health. If health damage occurs as a result of a healthcare professional´s misconduct, the question is whether there is liability for the misconduct in a given case and who is actually responsible.[23] Towards a healthcare professional, several types of liability may be imposed. In the field of private law, it will be *civil* and *labor law liability*, in the field of public law then *criminal liability, administrative liability* or it may be *disciplinary liability*. In the vast majority of cases, these are cases of liability for damage to health during the provision of health care. In civil proceedings, the defendant can be released from liability if he can prove that he was not responsible for the damage. The exception is the case of the so-called **objective responsibility** (responsibility for the result or strict liability).

For the purposes of this article, we will focus more closely on civil liability. From the point of view of the provision of health care, provision § 421a of the Civil Code is relevant - *everyone's responsibility for damage caused by circumstances that originate in the nature of the device or other thing that was used in fulfilling the obligation.* This type of liability can also arise if the health care was provided lege artis. This is an absolute objective responsibility that cannot be waived, even if the subject was not at fault. He will not bear it only if he proves that the damage was not caused at all. This is, for example, a situation where a defective incubator harms the health of a newborn baby or when a vaccine causes serious side effects to a patient. Therefore, in this sense, every case in which a medical device has failed will be considered. On the basis of these and other legal provisions, it is clear that in the event of an error in the provision of health care, the healthcare professional who caused it, or the healthcare provider. If there is an error related to a device working based on artificial intelligence, the question arises whether the provisions of Section 421a of the Civil Code will also apply to this case. There are two possibilities that differ in the degree of automation, namely, (i) either it will be a programmed robotic tool with elements of artificial intelligence, which the doctor uses like any other tool, but this tool has the functions of artificial intelligence that we mentioned above, for example, it detects tendons and stops the cut or (ii) it will be a fully autonomous robot that works by itself without human intervention. In both cases, the determination of responsibility will be the subject of a discussion, which must include an assessment of the extent to which the doctor was at fault and the extent to which the device/robot was faulty. According to strict liability, in the event of an adverse event associated with a device working based on artificial intelligence (i), the manufacturer, distributor or seller of the product may be liable, in accordance with provision 421a of the Civil Code, even if they were not responsible for the damage. In other words, even a system that has been well designed and implemented can still be liable for errors. This might appear to be a strict regulation, but it encourages continuous improvement in technologies that could remain disproportionately error-prone and based on outdated or unrepresentative data sets.[24] We believe that in the event that a surgeon provides medical care using a robot (with elements of artificial intelligence), it is an interplay of several factors and the use of provision 421a of the Civil Code will not be so simple. This is not "just a device that went wrong." We are talking about a situation where an error occurs during a surgical procedure, which will have a direct negative consequence on the patient's health and will be caused by the inconsistent cooperation between the surgeon and the robot - for example, the surgeon relied on the robot and his declared properties (e.g. detection of the presence of tendons), the surgeon could not proceed according to his own discretion (blocking by the robot) and therefore his late appropriate reaction and so on. In these cases, the regulation of the division of responsibility should be sufficiently elaborated, which will support the development of innovations and at the same time will not be abused

[22]Provision § 415 of Act no. 40/1964 Coll. Civil Code
[23]KOVAČ, Peter. The doctor's responsibility in providing health care. In: *Via Practica* , 2005, Vol. 2 (5), p. 272.
[24]PASQUALE, Frank. *When medical robots fail: Malpractice principles for an era of automation.* In: Teach Stream. Available at: https://www.brookings.edu/techstream/when-medical-robots-fail-malpractice-principles-for-an-era-of-automation/

by healthcare workers or technology companies. The second level of responsibility relates to fully autonomous robots (ii) that will be able to perform surgery without human assistance. Will the provision of 421a of the Civil Code be applied in this case?

4 CONCLUSION

In the second chapter of this article, we outlined the legal regulation of the provision of health care in the conditions of the Slovak Republic, including the entities that can provide it. It is a seemingly simple regulation, but the analysis of which is crucial for the needs of incorporating artificial intelligence in healthcare. If we are starting to think about autonomous robots, in addition to ethical and socio-economic aspects, legal ones also play an important role. Without their assessment and consideration, it will not be possible to think about artificial intelligence in healthcare on a practical level. In the article, we focused on the field of robots used in surgery, but artificial intelligence has a much wider scope in the provision of health care. In addition to robotic operations, we can talk, for example, about remote monitoring of a person's health attributes, which the system is able to analyze and, based on summarized results, recommend adequate treatment, or we can mention programs that determine possible and impossible drug interactions, and many other cases. The third chapter of the article focused precisely on the presentation of artificial intelligence and its possibilities in healthcare.

The most comprehensive analysis of the issue, which was the goal of this article, includes an assessment of legislation in general and legal liability in particular, which is also part of the legal arrangement, but it is necessary to look at it separately.

We consider two factors affecting legal liability of autonomous robots, whether this kind of artificial intelligence is a service or o product and how manual and limitations are communicated to the user / purchaser.

If we say that is a product, based on provision 421a of Civil Code, we will have several subject who could be held liable:

a) person who instructs robot,
b) person who programme robot (more options: the programmer, the programme designer, the expert who provides the knowledge, the manager who appointed inadequate expert, designer or programmer),
c) person who trains how to use robot.

In order to be able to answer sufficiently question of legal responsibility of robots, there are additional questions to be taken into consideration:

- If the user (healthcare professional) supplies the robot with additional parameters necessary for a specific operation of a specific person, should he be jointly responsible? Can we talk about shared responsibility?
- If the healthcare professional relied on the robot and its declared functions which did fail, will he be jointly responsible?
- What if the healthcare professional couldn't continue the operation because the robot got blocked and the doctor's autonomous reaction came thus late?

Slovak legislation currently does not allow to use autonomous robot in the position of healthcare professional. However, examples from abroad and activities of European Union show that using artificial inteligence in healt care if the future. Therefore, the legislation should sufficiently motivate technological companies to develop innovations and in the same time, it should not be abused by healthcare professionals.

This article was drafted with the support from a grant awarded by the Slovak Research and Development Agency No. APVV – 17 – 0403 Effects of Mutual Recognition of Electronic Identification Means on Electronic Services of Public Administration and is included in a research task.

References:

DOLIC, Zrinjka – CASTRO, Rosa – MOARCAS, Andrei. *Robots in healthcare: a solution or a problem?*, Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, 24 p., ISBN 978-92-846-4771-2.

GOMEZ-GONZÁLES, Emilio – GOMEZ-GUTIERREZ, Emilia. *Artificial Intelligence in Medicine and Healthcare: applications, availability and societal impact*. Luxembourg: Publications Office of the European Union, 2020, ISBN: 978-92-76-18454-6.

EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the* Regions on telemedicine for the benefit of patients, healthcare systems and society. Brussels, 2008, 14 p.

KOVÁČ, Peter. The doctor's responsibility in providing health care. In: *Via Practica* , 2005, Vol. 2 (5), p. 272.

PASQUALE, Frank. *When medical robots fail: Malpractice principles for an era of automation.* In: Teach Stream. Available at: https://www.brookings.edu/techstream/when-medical-robots-fail-malpractice-principles-for-an-era-of-automation/

STŘEDA, Leoš – HÁNA, Karel. *eHealth and telemedicine.* Prague: Grada Publishing, 2016, 160 p., ISBN 978-80-247-5764-3

Act no. 40/1964 Coll. Civil Code

Act no. 576/2004 Coll. on health care, services related to the provision of health care and on the amendment of certain laws

Act no. 578/2004 Coll. on health care providers, health professionals, and state organizations in the health sector and on the amendment of certain laws as amended by later legislation

UNITED NATIONS. Universal Declaration of Human Rights, 1948.

UNITED NATIONS. International Covenant on Economic, Social, and Cultural Rights, 1966.

COUNCIL OF EUROPE. Convention on Human Rights and Biomedicine, 1999.

Contact information:

Doc. JUDr. Soňa Sopúchová, Ph.D.
sona. sopuchova @ flaw.uniba.sk
Comenius University in Bratislava
Faculty of Law
Šafárikovo nám. 6, PO Box 313
810 00 Bratislava 1
Slovak Republic

NFT: POSSIBLE TECHNOLOGIC USES

Petra Žárská[1]

Comenius University, Faculty of Law

Abstract: NFTs or Non-fungible tokens might be possibly used in many ways. NFTs are based on the Blockchain technology. The artistic and technologic quality of NFTs make it the object of various legal regimes and various uses. NTFs might by regulated as crypto assets and authors' works at the same time. There is also a possible use for the identification of people within the digital world and closed national systems. NFTs are not currently specifically regulated in EU, therefore NFTs' authors and owners face unclear legal rights and obligations under at least two legal regimes.
The article will thoroughly analyze which legal regimes can be applied to NFTs. The article will be divided into four parts and summary. First part will enlighten the character of NFTs, the second part explores the applicability of crypto regulations of EU to NFTs. The third part will evaluate the possibility of the use for identification of persons in digital world. The fourth part will focus on risks and benefits of NFTs. The summary will be dedicated to the compact assessment of NFTs.

Key words: NFT, non-fungible token, crypto-asset, identification, copyright

1 INTRODUCTION

Non-fungible tokens (further also as "NFTs") is a new phenomenon in the digital world. NFTs have become a phenomenon for its increased use since 2018. Until 2018, NFTs were perceived as peculiar tokens known only to few experts and enthusiast of Blockchain. We can date the creation of a first NFT in 2014, when the artwork Quantum was created in the Blockchain Etherum.[2] Then the explosion of NFTs has started. "The total value of all NFT transactions in 2020 hit just over $250 million, almost four times the $62.9 million that was traded in 2019."[3] The most expensive NFT was sold on December 2, 2021 under the name The Merge for a total cost of $91.8m.

[1] Mgr. Petra Žárská PhD., LL.M., an assistant of professor at the Institute of Information of Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava. This article was created under research project APVV 17-0403: „Influence of mutual recognition of electronic identification means on public administration electronic services."

[2] *Theartnewspaper.com*. [online webpage]. Sotheby's and artist Kevin McCoy sued over sale of early NFT [cit. 2022-09-18]. Available at: https://www.theartnewspaper.com/2022/02/04/sothebys-kevin-mccoy-lawsuit-quantum-nft

[3] *Cloudwards.net*. [online webpage]. NFT Statistics, Facts & Trends in 2022: All You Need to Know About Non-Fungible Tokens. [cit. 2022-09-18]. Available at: https://www.cloudwards.net/nft-statistics/

The Merge by Pak

NFTs acquired a very intriguing reputation in the digital world. The reputation is the result of the opportunities that NFTs offers, its complex character and popular use as a storing of financial value.

The raising popularity of NFTs requires the closer look on the character of an NFT. What is a NFT? Currently, there is no legal definition of an NFT. Are you asking why? The reason is its minimal use in the past, when only a dozen of people knew about it and used it. Nowadays, the first kegal definition should be included in the MiCA Proposal. On September 24, 2020, the European Commission adopted a digital finance package that includes a legislative proposal for the regulation of crypto assets, the Markets in Crypto assets Regulation called also the MiCA Proposal. The MiCA Proposal includes regulations that would apply to NFTs in certain cases and defines for the first time in the EU a crypto asset as a "digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology".[4] We will have to wait for the binding legal definition of an NFT. Meanwhile, for the purpose of this article we can adopt a practical definition developed by the lack of legal definition. According to Clifford Chance, "an NFT is a digital asset whose uniqueness and ownership can be demonstrated and verified using distributed ledger technology (DLT)."[5]

2 THE USES OF NFTS

NFTs are hybrids because it can be considered an art, therefore potentially protected by Copyright, also a crypto asset and identification tool at the same time. NFTs cross at least two legal regimes.

2.1 The character of NFTs

How is an NFT created? Before we start to explain the creation of NFTs, we should enlighten few key terms such as DLT, blockchain and token. DLT or a distributed and decentralized ledger, is a non-proprietary technology that is used for establishing blockchain. "DLT such as Blockchain, the underlying technology for the first successful cryptocurrency—Bitcoin, is a system that offers immutable and secure processing and recording of transactions that can be anything of value across a distributed, decentralised, peer-to-peer network. Several types of DLT are available including public,

[4] Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/193, COM/2020/593 final.

[5] *Cliffordchance.com.* [online webpage]. NON-FUNGIBLE TOKENS: THE GLOBAL LEGAL IMPACT. [cit. 2022-09-18]. Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf. p. 2.

consortium and private; access can be permissioned or permissionless."[6] NFTs are part of blockchain in the form of a token. Token is a piece of a code of Blockchain. Before an physical object (paper photography) or digital object (digital photography) become an NFT, these object must be tokenized. For this article, we focus on the Etherum Blockchain, because it is the most popular blockchain for creating NFTs. The tokenization process is undertaking under two basic standards. The standard known as ERC-720 is used for the creation of fungible tokens such as bitcoins or other crypto currencies. Standard known as ERC-721 is used for the creation of non-fungible tokens. At this point of the creation process, we have two choices. Either we create NFTs by downloading these standards, which is for many people a bit complicated, or we can use so called "minting" platforms such as Opensea[7], Rarible[8] and many others. The easier choice is to mint an NFT via those platforms. The process of NFT creation starting from uploading a photography to a platform or to a standard is called "minting". "In this context, minting a work as an NFT means that a creator uses a digital work to generate a unique number that is then written into the blockchain in the shape of a smart contract using the ERC-721 standard, and this is done using a unique digital signature that belongs only to the person minting it. In principle, this is what gives the NFT its 'scarcity' value: it is supposed to be unique. In reality, anyone can mint as many versions of the same work as they wish."[9]

After the minting process, how the NFT look like? It can be viewed only online in the form URL link that takes us to the specific token within the Blockchain. As result, NFTs can be traded only online too. It is not a physical object like a sculpture or a coin. "The first core element to the NFT is a number known as the tokenID, which is generated upon the creation of the token; the second is the contact address, this is a blockchain address that can be viewed everywhere in the world using a blockchain scanner. The tokenID and the contract address are the most important elements, as they are linked specifically to both the original work and the signature used to generate the token."[10]

Who can create NFTs? Good news, anyone can create NFTs. Thanks to minting platforms, NFTs are becoming very popular among artists and non-artists as well.

2.2 NFT as a work protected by Copyright

NFTs are seen as a part of art, because usually the content of an NFT is visual, something that can be captured as a photography, text or video. Regarding authorship and authorial rights, an NFT can be created in two ways. First, the author of NFT is also the author of the basis of NFT – an image, text, video. Therefore, one person holds Copyright to the NFT and to the original work that is the content of NFT. The original work and NFT are not the same. The owner/creator of NFT also do not automatically hold Copyright to the original work unless she/he is not the author of the original work. For example, when you buy the original painting of Frida Kahlo, you are not automatically entitled to use the painting on t-shirts, mugs,... Also, when you buy the NFT, for example the NFT featuring a popular meme, you own only the NFT featuring a meme, but you do not own the original meme. Therefore, anyone can use the meme and you are not entitled to forbid its use by other people. When the owner owns an NFT or author created an NFT, they hold Copyright to the NFT, not to the original work. What about when you use for an NFT a work of someone else? Ideally, you are legally

[6] Li J., Kassem M. and Watson R. *A blockchain and smart contract-based framework to increase traceability of built assets.* In: Proc. 37th CIB W78 Information Technology for Construction Conference (CIB W78), São Paulo, Brazil, p. 349.

[7] *Opensea.io.* [online webpage]. Explore, collect, and sell NFTs. [cit. 2022-09-18]. Available at: https://opensea.io/

[8] *Rarible.com.* [online webpage]. Community-centric NFT marketplace. [cit. 2022-09-18]. Available at: https://rarible.com/

[9] Guadamuz A. *The treachery of images: non-fungible tokens and copyright.* In: Journal of Intellectual Property Law & Practice, 2021, jpab152, https://doi.org/10.1093/jiplp/jpab152, [cit. 2022-09-18]. Available at SSRN: https://ssrn.com/abstract=3905452 or http://dx.doi.org/10.2139/ssrn.3905452, p. 1370.

[10] Guadamuz A. *The treachery of images: non-fungible tokens and copyright.* In: Journal of Intellectual Property Law & Practice, 2021, jpab152, https://doi.org/10.1093/jiplp/jpab152, [cit. 2022-09-18]. Available at SSRN: https://ssrn.com/abstract=3905452 or http://dx.doi.org/10.2139/ssrn.3905452, p. 1371

obliged to acquire the consent of the author of this work. Many authors of NFTs do not acquire the consents and create NFTs without it. As result, many sold NFTs are counterfeits. NFTs are works protected by Copyright assuming that it has been created with consent of the author of original work or the author of the NFT and original work is the same person. Also, the original work must a work protected by Copyright, otherwise, Copyright protection is provided for the NFT based on this original work.

2.3 NFT as an identification tool

The use of NFT for identification of people is very new, the research in this area is limited. The identification of a person can be the identification in the physical world by the ID card or in the digital/online/virtual world by using again the ID card or password or other identificatory. NFTs can be used only digitally, therefore the identification in the digital world, within platforms or national administrative systems can be discussed. We can compare an NFT to a square code in the terms of identification in the digital world because the functional principle is the same. The same way as a square code function and give us required information, an NFT identify a person due to its uniqueness. The metaverse has been recently created. "The Metaverse is the post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital virtuality. It is based on the convergence of technologies that enable multisensory interactions with virtual environments, digital objects and people such as virtual reality (VR) and augmented reality (AR). Hence, the Metaverse is an interconnected web of social, networked immersive environments in persistent multiuser platforms. It enables seamless embodied user communication in real-time and dynamic interactions with digital artifacts. "[11] Although, this environment might be alien to many of us, there is a need for identification in it. How can we identify a person in the metaverse? "The answer may lie in non-fungible tokens (NFTs). These blockchain-based records of digital ownership have taken the world by storm due to the multi-million-dollar sales of digital art, memes and playing cards with which they have become synonymous. If a digital concert ticket can be programmed with unique ownership rights and stored in blockchain, so too can a virtual identity. To be sure, no technology can perfectly protect identity (NFT encryption keys might be stolen, for example). But the robustness of blockchain security, and the platform fluidity enabled by blockchain decentralisation, promise to transform the metaverse experience, by enabling established identities that can move freely between immersive virtual worlds. The NFT will enable people to demonstrate and have an identity across platforms that they can clearly own and use on different ecosystems. The fact that even the big digital platforms are starting to use that as an element to demonstrate your identity is very powerful."[12] NFTs will probably represent the whole digital identity of a person in the digital world thanks to its uniqueness, durableness, and proof of ownership by a person. „Identity in the Metaverse should be considered almost like a genetic code that confirms biological identity". That is, it should allow us to move through different environments within the Metaverse using a full-fledged alter ego."[13] We can compare the NFT identity proof to a human DNA in terms of accuracy and rely on the system of NFT identifiers in the digital world the same way as we rely on biologic identifiers in the physical world.

2.4 NFT as crypto asset

In EU, NFTs are not yet regulated. "While the EU extended its AML regulatory framework to include "virtual currency exchanges" and "custodian wallet providers" through its implementation of the AMLD5* in 2018, it did not define regulations specific to NFTs, most probably because NFTs,

[11] Mystakidis, S. *Metaverse.* In: Encyclopedia 2022, 2, 486–497, https://doi.org/10.3390/encyclopedia2010031. [cit. 2022-09-18]. Avaible at https://www.researchgate.net/publication/358497370_Metaverse, p. 486.

[12] *Ft.com*. [online webpage]. NFTs: Identity in the metaverse. [cit. 2022-09-18]. Available at: https://www.ft.com/partnercontent/crypto-com/nfts-identity-in-the-metaverse.html

[13] *Miteksystems.com.* [online webpage]. What is the Metaverse? [cit. 2022-09-18]. Available at: https://www.miteksystems.com/blog/what-is-the-metaverse?utm_source=twitter&utm_medium=social&utm_campaign=steve-ritter&utm_term=what-is-the-metaverse&utm_content=blog

although well known to crypto enthusiasts, were not widely being used."[14] As result, NFTs were left out of EU crypto regulations although, it is created the same way as crypto currencies only by using a different standard. According to press release of the Council of the EU, "non-fungible tokens (NFTs), i. e. digital assets representing real objects like art, music and videos, will be excluded from the scope except if they fall under existing crypto-asset categories. Within 18 months the European Commission will be tasked to prepare a comprehensive assessment and, if deemed necessary, a specific, proportionate, and horizontal legislative proposal to create a regime for NFTs and address the emerging risks of such new market."[15] The categories of NFTs which will fall under existing crypto-asset categories are unclear for now, we must wait for the proper definition of these categories. The further legislation on NFTs is expected in next 18 months, we can assume that until then, existing EU anti-money laundering rules will be applicable to sales of NFTs for an amount of €10,000 or more.

3 CONCLUSION

Owning NFTs brings many benefits such as securing a new type of valuable art, a new type of investment. If you take a part in metaverse, you might be identified in it by the NFT identifier. In metaverse, the whole identity of a party can be trusted to the NFT identity. The diverse use of NFTs brings also diverse legal rights and obligations under Copyright law, AML regulations and legal codes of EU members where is the identification considered. The NFT as crypto asset will be regulated partially by MiCA. The new specialised EU regulation on NFTs is under way. NFTs as a works of art protected by Copyright are already part of legal regimes. The future use of NFTs as identifiers and virtual identities is completely unregulated. Therefore, everyone who owns the NFT must consider Copyright protection, whether the NFT is worth more than 10,000 euros and be prepared for the use of NFT as identificatory in metaverse.

Bibliography:

Guadamuz A. *The treachery of images: non-fungible tokens and copyright.* In: Journal of Intellectual Property Law & Practice, 2021, jpab152, https://doi.org/10.1093/jiplp/jpab152, [cit. 2022-09-18]. Available at SSRN: https://ssrn.com/abstract=3905452 or http://dx.doi.org/10.2139/ssrn.3905452.
Li J., Kassem M. and Watson R. *A blockchain and smart contract-based framework to increase traceability of built assets.* In: Proc. 37th CIB W78 Information Technology for Construction Conference (CIB W78), São Paulo, Brazil.
Mystakidis, S. *Metaverse.* In: Encyclopedia 2022, 2, 486–497, https://doi.org/10.3390/ encyclopedia2010031. [cit. 2022-09-18]. Avaible at https://www.researchgate.net/publication/358497370_Metaverse.
EU law:
Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/193, COM/2020/593 final.

Online sources:

Consilium.europa.eu. [online webpage]. Digital finance: agreement reached on European crypto-assets regulation (MiCA) [cit. 2022-09-18]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

[14] *Skadden.com.* [online webpage]. What is the Metaverse? [cit. 2022-09-18]. Available at: https://www.skadden.com/insights/publications/2021/06/regulatory-approaches-to-nonfungible-tokens

[15] *Consilium.europa.eu*. [online webpage]. Digital finance: agreement reached on European crypto-assets regulation (MiCA) [cit. 2022-09-18]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

Cliffordchance.com. [online webpage]. NON-FUNGIBLE TOKENS: THE GLOBAL LEGAL IMPACT. [cit. 2022-09-18]. Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf

Cloudwards.net. [online webpage]. NFT Statistics, Facts & Trends in 2022: All You Need to Know About Non-Fungible Tokens. [cit. 2022-09-18]. Available at: https://www.cloudwards.net/nft-statistics/

Ft.com. [online webpage]. NFTs: Identity in the metaverse. [cit. 2022-09-18]. Available at: https://www.ft.com/partnercontent/crypto-com/nfts-identity-in-the-metaverse.html

Miteksystems.com. [online webpage]. What is the Metaverse? [cit. 2022-09-18]. Available at: https://www.miteksystems.com/blog/what-is-the-metaverse?utm_source=twitter&utm_medium=social&utm_campaign=steve-ritter&utm_term=what-is-the-metaverse&utm_content=blog

Opensea.io. [online webpage]. Explore, collect, and sell NFTs. [cit. 2022-09-18]. Available at: https://opensea.io/

Rarible.com. [online webpage]. Community-centric NFT marketplace. [cit. 2022-09-18]. Available at: https://rarible.com/

Skadden.com. [online webpage]. What is the Metaverse? [cit. 2022-09-18]. Available at: https://www.skadden.com/insights/publications/2021/06/regulatory-approaches-to-nonfungible-tokens

Contact information:
Mgr. Petra Žárská, LL.M., PhD.
petra.zarska@uniba.sk
Comenius University
Šafárikovo námestie č. 6
Bratislava
Slovakia

WHAT THE REVISION OF EIDAS BRINGS

Martin Daňko

Comenius University Bratislava, Faculty of Law

Abstract: This article analyses the revision of the eIDAS Regulation, which introduces new legal institutes in the field of cross-border electronic identification. The author looks in more detail at the electronic digital identity wallet, which could also bring new possibilities for cross-border electronic identification for the private sector.

Key words: eIDAS Regulation, European Digital Identity, European Digital Identity Wallets

1 INTRODUCTION

The possibilities of digital communication between the public and private sector actors across the EU also represent challenges to the development of legislation governing the digital interconnection of entities in the Single Market. The legislative process in this field can be described very easily, as Regulation (EU) No 910/2014 on electronic identification and services for electronic transactions in the internal market (the 'eIDAS Regulation') has laid the necessary legal basis for that call, and so that individuals and businesses can already participate digitally in public sector e-services in each Member State through that legislation.[1] This means that through the technological and legal possibility of digital identification implemented in their home country, which is recognized in other EU countries, the entities can communicate digitally using the eIDAS modified eID trust services. In a new proposal to revise the eIDAS Regulation, the European Union considers the existing options ensuring access only to public digital services to be insufficient. We have to state that since 2014 the situation has also changed in terms of the possibilities of using information and communication technologies, which is a sufficient reason to do more in electronic communication within the EU.

It is possible to do more if we manage to identify a way to achieve this, which in the context in question primarily means eliminating the shortcomings of the eIDAS regulation, which prevents greater use of electronic communication in the construction of the internal market. The evaluation in question is based on the European Commission's document entitled 'Europe's Digital Decade: 2030 Digital Targets', which states Inter alia that by 2030 up to 80% of EU citizens will use digital identification.[2] It is therefore clear that the future of the EU will depend on digital skills, for the realization of which a generally recognized public e-identity is needed in the EU space.[3] An electronic

[1] See ANDRAŠKO, J.: Vybrané aplikačné problémy vzájomného uznávania prostriedkov elektronickej identifikácie v zmysle nariadenia eIDAS. Míľniky práva v stredoeurópskom priestore 2019 [electronic document]. - : 1. vyd. ISBN 978-80-7160-517-1. - Bratislava : Právnická fakulta UK, 2019. - p. 387-396 [online], DUMORTIER, J.: Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). [online] Available at SSRN: https://ssrn.com/abstract=2855484 or http://dx.doi.org/10.2139/ssrn.2855484.

[2] On March 9, 2021, the European Commission presented the vision and ways to achieve the digital transformation of Europe by 2030. See more online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital- age/europes-digital-decade-digital-targets-2030_en. These visions were embodied by the European Parliament and the Council in the Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the 2030 Policy Programme “Path to the Digital Decade“, Brussels, 15/09/2021, COM (2021) 574 final, 2021/0293 (COD) (hereinafter ""Path to the Digital Decade“. Available online: https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52021PC0574&qid=1657184403339.

[3] TENHUNEN, S.: Revision of the eIDAS Regulation. Findings on its implementation and application. European Parliamentary Research Service; PE 699.491 – March 2022, s. 2, Available online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491.

identity for everyone, through available information and communication technologies, should be part of a digital environment that is easy to use, efficient and uses personalized services and tools with high security and privacy standards.[4]

2 REVISION CONTENT

The changes to be brought about by the revision of the eIDAS Regulation are based on the shortcomings of existing legislation on digital identity and trust services, while also underlining the desired effect of these changes on the needs of the internal market. It is precisely the internal market, that is supposed to facilitate cross-border electronic services using digital identity in the digital environment, thereby increasing the scope for electronic transactions that have not been possible until now due to the absence of cross-border provision of electronic identification in the private sector. Cross-border electronic services can only exist for digital identity identification and authentication with a high level of trust for the communicating parties. Only users' trust in the services providing their digital communication brings trust in all electronic communication processes.

The need for users and the internal market is the reason why the revision of the Regulation must provide solutions ensuring access to trustworthy and secure solutions for the cross-border use of digital identities. Users are increasingly accustomed to globally available solutions, for example when they accept the use of single login system solutions provided by larger social media platforms to access online services. Member States themselves cannot solve the problems that arise as a result in terms of the market power of large providers, which requires interoperability and trustworthy electronic identifications at the EU level. Electronic attribute certificates issued and accepted in one Member State, such as an electronic health certificate, are often not legally recognized or accepted in the other Member States.[5]

2.1 Electronic attestation of attributes

The upcoming changes will also bring a new perspective on the possibilities of sharing electronic attribute certificates. Attributes contain information about the characteristics of the entity, which in the case of a natural person is their legal name and surname or date of birth, as well as details from other organizations about the entity, such as professional qualifications, bank balance, or medical history. Digital identities[6] shall also consist of such characteristics or attributes belonging to a natural person, legal person or electronic device. The information contained in the digital identity allows the user to authenticate or present their digital attributes, allowing them to access public or private services online or offline.[7] Where such attribute can be certified by a third party that will be legally entitled to its certification authority, in which case the use of certified attributes in cross-border electronic communications is possible. The use of certified attributes can not only shift to other spheres of public services but cross-border electronic communications can also be used for services provided by the private sector. Any fact that can be verified by means of the information contained in the certified attribute of the electronic identity of the entity has caused the removal of barriers to the

[4] Recital 89 Path to the Digital Decade.

[5] See Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, EUROPEAN COMMISSION Brussels, 3.6.2021 COM (2021) 281 final 2021/0136 (COD), (hereinafter "Proposal of revision eIDAS"), paragraph 2, Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[6] See ANDRAŠKO, J.: Elektronická identita In. Právo informačných a komunikačných technológií : 1. - : 1. vyd. ISBN 978-80-973837-0-1. - Bratislava : TINCT, 2020. - S. 178-217, SULLIVAN, C.: Is Your Digital Identity Property? An examination of digital identity in the era or e-government and digital citizenship. In. European Property Law Journal; Berlin Vol. 2, Iss. 2, (2013)

[7] See The UK digital identity and attributes trust framework. Available online: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework.

use of cross-border electronic services, the provision of which depends on the provision of information through trust services.

The draft regulation regulates in Article 45a the legal effects of electronically certifying attributes in the form of their admissibility as evidence in legal proceedings, as well as the impossibility of refusing them solely because of their existence in electronic form. Article 45a of the revised draft provides for the same legal effect for a qualified electronic certificate of attributes as certificates legally issued in paper form and stipulates that, if such a certificate is issued in one Member State, it is recognized as a qualified electronic certificate of attributes in any other Member State.

2.2 Certificate services for website authentications

In order to ensure the trust and security of the cross-border digital identity solution and citizens' full control over their personal data, the revision of the eIDAS Regulation also provides a legal framework for certification services for website authentication. The motives for the new regulation are based on ensuring a state of security for the user of the website, in which the user trusts the entity acting as an entrepreneur. Digital communication between the website user and the entities operating the website also requires the existence of a sufficient number of guarantees that confirm that the entrepreneur is a real and legitimate entity. The idea of the drafters of the revision of the eIDAS Regulation is to create user confidence in a verified website through the fact that there is an authority that has the power to verify its authenticity.

In terms of content, the review introduces at least obligations regarding the security and liability of providers of authentication of websites and their services. On the other hand, this also entails obligations for web browsers by ensuring support for, and interoperability with, qualified website authentication certificates. This requirement imposed by a web browser is derived from the need to be able to recognize and display qualified website authentication certificates and to enable:

a. website owners to identify themselves as website owners, and
b. identify website owners with a high degree of certainty to users.

According to Article 45 of the revised proposal, this objective can be achieved by ensuring the requirements for qualified certificates for website authentication set out in Annex IV to the eIDAS Regulation and the obligation for web browsers to recognize, support and display the website identity data in a user-friendly manner. We believe that the obligations thus laid down for web browsers are an adequate reason to develop additional costs for technologically necessary processes, given the context of the intention, i.e. to create opportunities for better authentication of website operators. Under optimal circumstances, this may also mean some market pressure on web browsers to provide functionality from the aforementioned web authentication needs.

2.3 Electronic archivings

Another beneficial legal institution found in the analyzed revision of the eIDAS Regulation is electronic archiving[8], the main objective of which is to enable the long-term preservation of electronic documents and related trust services. In view of the proposed obligations, electronic archiving will affect the Member States, which must introduce national requirements for services providing secure and trustworthy digital archiving.[9] The proposal for a revised regulation materializes the requirement of trust in the use of cross-border electronic communications also in the form of regulation for the cross-border recognition of qualified electronic archiving services. The Explanatory Memorandum to

[8] See HODOSSY, K.: Cloud services and their impact on Slovak e-Government. Security risk or not? In. Míľniky práva v stredoeurópskom priestore 2020 [elektronický dokument] : zborník z online medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov. - : 1. vyd. ISBN 978-80-7160-576-8. - Bratislava : Právnická fakulta UK, 2020. - p. 711-719 [online].

[9] ŽÁRSKÁ, P.: Databases in the electronic identification and authentication system: lawful use of personal data. In. Acta Facultatis Iuridicae Universitatis Comenianae. - Vol. 39, Iss. 2 (2020), p. 383-395.

the draft regulation sees this framework as an opportunity for trust service providers in the EU to open up new market opportunities.[10]

According to Article 3 pt. 16 of the draft revised Regulation, electronic archiving of electronic documents is considered a trusted service. The content of this service is to ensure the reception, storage, erasure, and transmission of electronic data or documents in order to guarantee, throughout the retention period, their integrity, the correctness of their origin, and their legal elements. Article 45g of the draft revised Regulation provides for a higher degree of trust in that service since the service in question can only be provided by a qualified trust service provider who uses procedures and technologies to extend the trustworthiness of an electronic document beyond its technological validity.

In connection with the above, it is necessary to mention the legal framework for new trust services, on the basis of which electronic registers and qualified electronic registers will be created and maintained. The electronic register[11] shall constitute an electronic record of data secured against tampering, ensuring the authenticity and integrity of the data and containing the correctness of the date and time of the recording of those data as well as the correctness of their chronological arrangement. On the question of the legal effect of an electronic register, the proposal for a revised Regulation, in a standard manner, sets out in Article 45h its nature as evidence in legal proceedings, which may not be rejected solely on the grounds that it has an electronic form or that it does not meet the requirements for qualified electronic registers and there is a presumption of the uniqueness and authenticity of the data it contains, the correctness of their date and time and their sequential chronological arrangement within that register. A qualified electronic register enjoys a higher degree of trust, which is reflected in the requirements for its existence laid down in Article 45i of the draft eIDAS Regulation.[12]

2.4 Qualified trust service provider

Public and private services can only be successful if the EU legal framework can ensure a sufficient level of trust and security when using a cross-border digital identity. Among other things, this also means giving users full control over their personal data and ensuring their security when using digital identity solutions.[13] From a legal point of view, it is a task to ensure a level playing field for the provision and acceptance of qualified trust services in the EU.[14] Those objectives can be achieved by imposing requirements on all qualified and non-qualified trust service providers for the secure exchange of identity data established in the EU by:

a. identity-related data functionally separated from activity data and other personal data on transactions or behavior or data obtained from third parties that are not directly related to the provision of the service will be provided;
b. offers the user the possibility to choose for each use of identity data for different or different purposes, together with clear information for the user on how and by whom this data will be used.

[10] Recital 33 of Proposal of revision eIDAS.
[11] According to Art. 3 letters l) point 53 of the draft of the new eIDAS regulation.
[12] According to Art. 45i of the draft eIDAS regulation,
1. Qualified electronic ledgers shall meet the following requirements:
(a)they are created by one or more qualified trust service provider or providers;
(b)they ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger;
(c)they ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry;
(d)they record data in such a way that any subsequent change to the data is immediately detectable.
[13] MESARČÍK, M.: Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov. In. Acta Facultatis Iuridicae Universitatis Comenianae. - Vol. 36, Iss. 2 (2017), p. 204-217.
[14] TENHUNEN, S.: Revision of the eIDAS Regulation. Findings on its implementation and application. European Parliamentary Research Service; PE 699.491 – March 2022, p. 8.

For qualified providers of such services, the rule shall apply whereby the provision of identity data is structurally separated from activity data and other personal data on transactions or behaviour or data obtained from third parties not directly related to the provision of the service.[15] Any measures for qualified and non-qualified trust service providers must reflect the rules set out in the GDPR, as the GDPR also provides individuals with the right to withdraw consent to the processing of their data. [16]

2.5 European Digital Identity Wallets

The proposal for a revised eIDAS Regulation answers the questions of the direction of further legislative changes in the field of cross-border electronic identification and the related provision of trusted service in the modification of a new legal institute called the European Digital Identity Wallet (EDIW). Despite the term legal institution used, it must be concluded that the revision of the eIDAS Regulation will create legal possibilities for the functioning of the product and services associated with it, which the user, under the name European Digital Identity Wallet, will use to digitally store identity data and attestations and attributes associated with his or her digital identity.[17] Article 6a(1) of the eIDAS proposal itself establishes EDIW as a trusted digital means serving in the EU space to ensure secure and seamless access by its user to cross-border public and private services for the use of which an eID is required.

This new electronic identification means a common interface for qualified and non-qualified trust service providers.[18] Following the adoption of the draft eIDAS Regulation, the trust service provider will be able to issue both qualified and non-qualified electronic certificate attributes or other certificates. Subsequently, trust service providers will be able to provide the attributes and certificates in question to the user, who uploads them to EDIW. The latter shall then submit them, as appropriate, to the relying parties, who shall validate the personal identification data and electronic certificates for the procedures and activities used to provide the electronic service. Since the provision of electronic services is also possible offline,[19] EDIW is a means by which the user submits personal identification data, electronic attribute certificates or other data without the need to access the Internet. However, in this case, the relying party must have the ability to validate the information provided offline.

From the point of view of personal data protection, it is important for the user that there is a technical solution that does not allow the provider of trust services of qualified attribute certificates to

---

[15] „Structural separation would provide users (people and businesses) the necessary reassurance that their data is safe under all circumstances and no additional combination / profiling is possible. It also enhances trust in ensuring that the identity data is not "sold" (beyond where legal obligations/possibilities exist) or traded for commercial purposes. Overall, structural separation would create the necessary trust to ensure uptake and usage of the system by people and businesses. For corporate users, full data security is a commercial and competitive requirement and needs to be ensured particularly for data generated by IoT devices." COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity SWD/2021/124 final, Paragraph 5, Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2021:124:FIN

[16] See ANDRAŠKO, J. a MESARČÍK, M.: Those Who Shall Be Identified: The Data Protection Aspect of the Legal Framework for Electronic Identification in the European Union. TalTech journal of European studies [electronical document]. - Vol. 11, Iss. 2 (2021), p. 4-24

[17] Article 3 point 42 of Proposal of revision eIDAS.

[18] Article 6a point 4 of Proposal of revision eIDAS.

[19] In the Slovak legal system, Standards of electronic public administration services according to § 34 letter a) point. 1 of the Decree of the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization on Standards for Public Administration Information Technology No. 78/2020 Coll. on standards for public administration information technologies establish the division of public administration electronic services according to the level of electroncilization into six levels, where level 0 is a defined public administration electronic service that is not electronically available online.

obtain information for the purpose for which individual attributes have been used, in other words, EDIW is only a means of ensuring the validity of the user's authentication and the electronic attributes provided by him. Article 6a(4)(c) of the eIDAS proposal requires EPDI that the assurance level of electronic identification schemes under Article 8 of the eIDAS Regulation be set 'high', in particular when it concerns the requirement for proof and verification of identity and for the management and authentication of electronic identification means. Consequently, Article 6a(4)(e) of the draft regulation lays down an obligation for EDIW to contain the minimum set of personal identification data necessary for the unique and permanent representation of a natural or legal person and to represent the natural or legal person concerned unambiguously and permanently. EDIW should bring its user control over the information it uses for online or offline authentication. The user may request and obtain, store, withdraw, combine and share personally identifiable data and electronic attribute certificates without having doubts about the protection of the processed data. This possibility shall be exercised by the user in a manner that is transparent and traceable[20] in relation to the purpose of using the electronic services.[21]

The issuing of an EDIW is the responsibility of each Member State, and a Member State may, within the meaning of Article 6a(2) of the draft regulation, do so itself through its authorities or entrust another entity to issue EDIW to the contracting Member State after fulfilling the legal and technical criteria laid down for the activity in question. Another option is for the independent entity that will issue the EDIW to be recognized by the Member State concerned to carry out such an activity. The Member State only has to provide for the validation process as a specific process provided for in Article 3(41) of the draft regulation, which takes place the process of verifying and confirming that the electronic signature or electronic seal or electronic certificate of attributes is valid. The European Digital Identity Wallet will be used to create a signature using a qualified electronic signature, and this is where the responsible role of the Member States to provide validation mechanisms for EDIW, in accordance with Article 6(5) of the draft regulation, comes in. It is these mechanisms that will ensure that relying parties and qualified trust service providers can verify the authenticity and validity of the identification data presented to users.

If the most significant benefits of the revision of the eIDAS Regulation were to be sought, this would undoubtedly include the issue of the cross-border use of EDIW. It is the unifying nature of the proposed legislation that is the most optimal means of creating a cross-border electronic identification means capable of ensuring access to cross-border electronic online services of both the public and private sectors. It is the relying parties of the private sector who can thus provide cross-border services, for the use of which strong user authentication is required. The legal grounding of this idea can be found in Article 12b(2) of the eIDAS proposal, which sets out an obligation for private relying parties. Where private parties provide services requiring the use of strong user authentication for online identification, or where strong user authentication is required by a contractual obligation, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, such private relying parties are obliged to accept the use of EDIW. In cases of cross-border use of EDIW on very large online platforms, where these platforms require users to authenticate when accessing online services, the draft revision provides, Article 12b(3) of the draft revision of eIDAS, provides the voluntary use of EDIW, where, at the voluntary request of the user on the other side of the platform, it is mandatory to accept the use of European digital identity wallets. Users should not be obliged to use the wallet to access private services, but very large online platforms should accept a European digital identity wallet for this purpose. Very large online platforms should respect the principle of data minimization when using EDIW. Given the importance of very large online platforms in terms of their reach, in particular in terms of the number of recipients of services and economic transactions, this is

[20] According to recital 33 of the proposal for a revised eIDAS Regulation, in order to ensure legal certainty and trust, it is essential to provide a legal framework to facilitate the cross-border recognition of qualified electronic archiving services. The reason for such a framework is for EU law to create the preconditions for the traceability of the use of electronic services, which is possible through services providing secure and trustworthy digital archiving allowing for the long-term storage of electronic documents and information about the trust services provided.

[21] Article 6a point 3 of Proposal of revision eIDAS.

necessary to increase the protection of users against fraud and to ensure a high level of data protection. [22]

3 CONCLUSION

In conclusion, two important facts should be mentioned. The first is the contribution of the revision in question, which could be of interest to the private sector. Through a digital identity e-wallet, it would be possible to shift the possibilities of cross-border electronic identification also to the design of the desired areas of the private sector. In our opinion, the idea that cross-border identification means should not be restricted only by public sector e-services is what can bring a whole new impetus to the improvement of the internal market is correct. However, it is important how this idea is implemented.

Secondly, the revision reflects the need for coherence of legislation in this area across Member States. Because only high-quality legislation can give all actors the opportunity to engage in building a technically, financially and administratively demanding task, such as the creation and functioning of an EDIW.

Bibliiography:

- ANDRAŠKO, J.: Elektronická identita In. Právo informačných a komunikačných technológií : 1. - : 1. vyd. ISBN 978-80-973837-0-1. - Bratislava : TINCT, 2020. - S. 178-217.
- ANDRAŠKO, J.: Vybrané aplikačné problémy vzájomného uznávania prostriedkov elektronickej identifikácie v zmysle nariadenia eIDAS. Míľniky práva v stredoeurópskom priestore 2019 [electronic document]. - : 1. vyd. ISBN 978-80-7160-517-1. - Bratislava: Právnická fakulta UK, 2019. - p. 387-396 [online].
- ANDRAŠKO, J. a MESARČÍK, M.: Those Who Shall Be Identified: The Data Protection Aspect of the Legal Framework for Electronic Identification in the European Union. TalTech journal of European studies [electronical document]. - Vol. 11, Iss. 2 (2021), p. 4-24
- DUMORTIER, J.: Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). [online] Available at SSRN: https://ssrn.com/abstract=2855484 or http://dx.doi.org/10.2139/ssrn.2855484.
- HODOSSY, K.: Cloud services and their impact on Slovak e-Government. Security risk or not? In. Míľniky práva v stredoeurópskom priestore 2020 [elektronický dokument]: zborník z online medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov. - : 1. vyd. ISBN 978-80-7160-576-8. - Bratislava : Právnická fakulta UK, 2020. - p. 711-719 [online].
- MESARČÍK, M.: Naozaj sa bojím tmy? Zopár úvah o technologickom determinizme v kontexte ochrany osobných údajov. In. Acta Facultatis Iuridicae Universitatis Comenianae. - Vol. 36, Iss. 2 (2017), p. 204-217.
- SULLIVAN, C.: Is Your Digital Identity Property? An examination of digital identity in the era or e-government and digital citizenship. In. European Property Law Journal; Berlin Vol. 2, Iss. 2, (2013) See The UK digital identity and attributes trust framework. Available online: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework.
- TENHUNEN, S.: Revision of the eIDAS Regulation. Findings on its implementation and application. European Parliamentary Research Service; PE 699.491 – March 2022, p. 8.
- ŽÁRSKÁ, P.: Databases in the electronic identification and authentication system: lawful use of personal data. In. Acta Facultatis Iuridicae Universitatis Comenianae. - Vol. 39, Iss. 2 (2020), p. 383-395.

[22] Recital 28 of Proposal of revision eIDAS.

Contact information:
doc. Mgr. Martin Daňko, PhD.
danko3@uniba.sk
Comenius University Bratislava, Faculty of Law Address
Šafárikovo nám. č. 6
810 00 Bratislava
Slovakia

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave