Application of artificial intelligence (AI) in the assessment of the credibility of statements in the cross-border taking of evidence in civil and commercial matters

by **Jura Golub***

Abstract: Regulation (EU) 2020/1783 on 'co-operation between the courts of the Member States in the taking of evidence in civil and commercial matters' introduces taking evidence by videoconference or other distance communications technology as the "gold standard" in the process of direct cross-border taking of evidence by examining a person who is present in another Member State. This represents a step forward compared to the previous Regulation 1206/2001, as the provision for direct evidence taking through videoconferencing was rarely applied in practice. The direct taking of evidence through videoconference contributes significantly to the realisation of the principle of orality and immediacy in civil proceedings, as opposed to indirect methods of cross-border taking of collection. On the other hand, a question arises whether the principle of immediacy is weakened by using videoconferencing, given that there is a "digital barrier" between a witness and the court. When assessing the credibility of the statements made by parties, witnesses, and experts, psychological criteria in addition to logical criteria plays an important role in shaping the court's opinion on the truth of the assertion regarding the existence of certain facts. As a solution for consideration, there is a possibility of using an artificial intelligence system to detect deception during the direct taking of evidence by examining parties, witnesses, or experts. However, the admissibility of the above solution should be considered as a multi-faceted issue, particularly regarding aspects of the right to a fair trial, personal data protection rules, and the proposed provisions of the Artificial Intelligence Act.

Keywords: cross-border taking of evidence, judicial cooperation in civil and commercial matters, artificial intelligence, civil procedure, statement credibility, deception detection

Recommended citation: Jura Golub, Application of artificial intelligence (AI) in the assessment of the credibility of statements in the cross-border taking of evidence in civil and commercial matters, 14 (2023) JIPITEC 376 para 1

A. Introductory considerations

1 This forward-looking paper addresses the potential use of artificial intelligence as an auxiliary tool for the court to assess the credibility of statements in the cross-border taking of evidence in civil and commercial matters. In general, the assessment of the credibility of statements by using various technology tools occupies the attention of the scientific public in the field of criminal procedural law. EU procedural law is generally opposed to the use of tools such as polygraphs for assessing the credibility of statements in court proceedings.[1] However, the normative activity of the EU in the field of cross-border taking of evidence in civil and commercial matters coupled with the development

* Jura Golub, LLM, PhD Student and Research Assistant, University of Osijek – Faculty of Law Osijek, S. Radića 13, HR - 31000 Osijek, Croatia; E-mail: jgolub@pravos.hr, ORCID: https://orcid.org/0000-0002-2440-8081.

1 Robert Bradshaw, "Deception and detection: the use of technology in assessing witness credibility" [2021] 37 *Arbitration International* 711.

of systems for assessing the credibility of statements based on artificial intelligence make it necessary to consider the potential of using such systems. Taking evidence in any judicial proceeding is a prerequisite for establishing the facts of the case and thus for the correct application of substantive law. To achieve this, it is crucial to ensure access to evidence, which contributes to the actualization of the right of access to justice.[2] In civil disputes with a cross-border element, access to evidence is even more challenging, especially in the context of taking evidence by way of examination parties, witnesses, or experts. Long distances and considerable travel costs mean that a balance must be struck between the principles of economy and efficiency and the principle of immediacy when choosing the method of the cross-border taking of evidence.[3] In this balancing act, the courts of the Member States applying Council Regulation (EC) No 1206/2001 of 28 May 2001 on 'cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters[4]' (hereinafter: Regulation 1206/2001) have usually opted for the method of indirect taking of evidence. According to data provided by the European Commission, during the mentioned period, in an average of 87.5% of cases, the court of one Member State requested the taking of evidence by the court of another Member State (the indirect taking of evidence), while in an average of 12.5% of cases, the direct taking of evidence was applied.[5] It is obvious that the direct method of taking evidence has failed with the application of Regulation 1206/2001, and thus the principle of immediacy as one of the fundamental principles of civil procedure.

2 In light of the identified shortcomings, Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on 'cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters[6]' (hereinafter: the Revised Evidence Regulation or RER) was adopted and entered into force on 1 July 2022. The RER, *inter alia*, introduces the use of videoconferencing or other distance communications technology as the "gold standard" in the direct taking of evidence by examining persons from other Member States, with the aim of strengthening access to justice,[7] and of facilitating and speeding up the taking of evidence.[8]

3 The introduction of videoconferencing as the primary method of direct taking of evidence by examining a person has undoubtedly strengthened the principle of immediacy. However, it is necessary to consider whether this represents significant progress in strengthening immediacy as a principle of civil procedure and whether there is room for further improvement, especially when considering the development of modern technology. In particular artificial intelligence systems developed for the purpose of deception detection. Indeed, the available research shows that humans are able to detect deception, i.e., untrue statements, in only 57% of cases.[9] Given that there is a kind of "digital barrier" between the court that takes evidence directly by way of videoconferencing and the person being heard, it can be assumed that the judge's perception is further weakened when assessing the credibility of statements, even though the examination takes place in real time with audio and visual production. To date, several applicable AI-based deception detection solutions have been developed. Typically, the systems analyse facial micro expressions and eye tracking, and perform verbal and linguistic

2 European Law Institute and UNIDROIT (eds), *ELI – Unidroit Model European Rules of Civil Procedure* (OUP 2021) 136.

3 Commission, "COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters" SWD (2018) 285 final, 29.

4 Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters [2001] OJ L 174/1 (hereinafter: Regulation 1206/2001)

5 Commission, "COMMISSION STAFF WORKING DOCUMENT EVALUATION Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters" SWD [2018], 11.

6 Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) (recast) [2020] OJ L 405/1 (hereinafter: Revised Evidence Regulation or RER)

7 Commission, "Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters" COM (2018) N 388 final, 6.

8 Revised Evidence Regulation, recital 21.

9 Bradshaw (n 1) 714. According to Amit Katwala, "The Race to Create a Perfect Lie Detector – and the Dangers of Succeeding" *The Guardian* (London, 5 September 2019)

analysis of respondents.[10] Based on this, AI and machine learning are used in an automated process to evaluate the credibility of a single statement, thus eliminating any subjective human influence.[11] Individual AI-based deception detection systems are explained in detail in the next sections of this paper.

4 Considering the above, the main research question is whether artificial intelligence can contribute to strengthening the principle of immediacy in the cross-border taking of evidence through videoconferencing. In this context, the paper aims to determine the admissibility of the application of AI in assessing statement credibility in the cross-border taking of evidence, and this must be viewed as a multi-faceted issue. First, it is necessary to legally qualify the position of the system for assessing statement credibility in court proceedings. Can a deception detection system be considered a *sui generis* witness or expert, or something else? Furthermore, the admissibility of the application of AI in the assessment of statement credibility via videoconferencing must be examined from the perspective of the right to a fair trial guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms[12] (ECHR), the Charter of Fundamental Rights of the European Union[13] (CFR), the General Data Protection Regulation[14] (GDPR), and the conformity of the application with the draft Artificial Intelligence Act[15] (AI Act).

B. EU normative framework for the cross-border taking of evidence in civil and commercial matters using videoconferencing.

5 The legal basis for the regulation of the cross-border taking of evidence in the EU is Article 81(2)(d) of the Treaty on the Functioning of the European Union,[16] and thus the RER is an integral part of the normative framework of the European Union in the area of judicial cooperation in civil and commercial matters.[17] The aim of the European approach to the regulation of the cross-border taking of evidence is to create an appropriate legal and procedural framework that complements the effective resolution of cases with cross-border implications, i.e., the successful application of European private international law.[18] In addition to this purpose, a uniform legal and procedural framework for cross-border taking of evidence is important for the functioning of the internal market of the European Union.[19]

6 Prior to the implementation of the RER, Regulation 1206/2001 was applied in cross-border taking of evidence in civil and commercial matters.[20] In the context of this issue, it should be noted that Regulation 1206/2001, "coyly" and as an incentive, provided the possibility for direct taking of evidence by videoconferencing by the requesting court.[21] However, this possibility was rarely used in

10 Bradshaw (n 1) 709.

11 ibid

12 Consolidated Version of the Europan Convention on Human Rights [2021] <https://www.echr.coe.int/documents/convention_eng.pdf> accessed 24 July 2022 (hereinafter: ECHR)

13 Charter of Fundamental Rights of the European Union [2016] OJ C202/389 (hereinafter: CFR)

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L119/1 (hereinafter: GDPR)

15 Commission, „Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" COM (2021) 206 final (hereinafter: AI Act)

16 Consolidated version of the Treaty on the Functioning of the European Union [2007] OJ C 202/1

17 Mirela Župan, "50 godina europske pravosudne suradnje u građanskim stvarima – 5 godina hrvatske primjene" [2019] 10(1) Godišnjak Akademije pravnih znanosti Hrvatske 475-476 <https://doi.org/10.32984/gapzh.10.1.20> accessed 25 July 2022

18 ibid 475-76.

19 Paula Poretti, "Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters as a guarantee of the right to effective judicial protection" in Željka Primorac et al. (eds), *Economic and Social Development - 16th International Scientific Conference on Economic and Social Development – "The Legal Challenges of Modern World"* (Varazdin Development and Entrepreneurship Agency, Faculty of Law – University of Split and University North 2016) 219 <https://bib.irb.hr/datoteka/833529.esd_Book_of_Proceedings_Split_2016_Online.pdf> accessed 28 July 2022

20 Revised Evidence Regulation, art 34(1)

21 Jiri Valdhans and David Sehnalek, "The 1970 Hague Evidence

practice. In the previous section, it was statistically established that the direct taking of evidence was used in only 12.5% of cases that required cross-border taking of evidence.[22] However, the European Commission estimates that videoconferencing was specifically used in only 10-25% of cases where the direct method of taking evidence was applied.[23]

7 In light of this, the RER replaces Regulation 1206/2001 and takes a digital step forward, by introducing a number of solutions related to electronic communication between the Member State authorities, evidence transfer and the legal effect of electronic documents, and the use of videoconferencing in the context of the direct taking of evidence.[24] The RER *ratione materiae* applies in civil and commercial matters when the court of one Member State requests the competent court of another Member State to take evidence or when it requests the direct taking of evidence in another Member State.[25] The Revised Evidence Regulation applies *ratione teritorii* in all EU Member States, with the exception of Denmark.[26]

8 Since this paper focuses thematically on the possible application of AI in the direct cross-border taking of evidence by videoconference, it is necessary to consider the relevant provisions of the RER on this method of taking evidence. In relation to Regulation 1206/2001, the RER more imperatively mandates the use of videoconferencing or other distance communications technology when a court in one Member State requires the direct taking of evidence by examining a person located in another Member State.[27] It further requires that such taking of evidence shall be conducted on the condition that this technology is available to the court and if the court considers it to be appropriate in light of the particular circumstances of the case.[28] A court of a Member State that wishes to hear a person located in another Member State using videoconferencing submits a request to the central body or the competent authority of another Member State using an appropriate form.[29] The RER does not provide details of the procedure of examination held through videoconferencing, but refers the courts or the authorities of the Member States to mutual agreements regarding practical arrangements for the examination[30] Therefore, in any other situation, the general provisions on direct taking of evidence in Article 19 of the RER should apply to the procedure of direct taking of evidence by examining persons through videoconference. The direct taking of evidence is always carried out on a voluntary basis without the use of coercive measures, and the person being heard must be informed of this.[31] A decision on the request for the direct taking of evidence is made by the central body or the competent authority of the requested Member State, and the RER prescribes the time limits for the decision on the request.[32] In the event that the request for the direct taking of evidence is not decided within the prescribed time limit, the RER also provides for a positive presumption that the request shall be deemed to have been accepted. The central body orcompetent authority of the requested Member State has the power to refuse a request only in certain cases, i.e., if a request for the direct taking of evidence does not fall within the scope of the RER, if a request does not contain all the information required by the RER (Article 5), or if the direct taking of evidence is requested in a manner that is contrary to the fundamental principles of law of the requested Member State.[33]

9 It should be noted that the RER proposal explicitly mentions that the examination of a person conducted by videoconference must take place on court premises.[34] However, in the adopted version of the RER, such a provision was not explicitly included, which opens the possibility of further broad interpretations regarding where a person is heard. Nevertheless, it can be interpreted from

Convention, the European Union and the 2001 EU Evidence Regulation – Interfaces" in C.H. van Rhee and Alan Uzelac (eds), *Evidence in Cross Border Civil Litigation* (Intersentia 2015) 359.

22 See n 5.

23 Commission (n 5) 45.

24 Elena Alina Ontanu, "Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure" (2022) 12(3) Oñati Socio-Legal Series 594 <https://opo.iisj.net/index.php/osls/article/view/1370> accessed 28 July 2022. See also Revised Evidence Regulation, arts 7, 8, 20. Revised Evidence Regulation, arts 7, 8, and 20.

25 Revised Evidence Regulation, art 1.

26 ibid recital 38.

27 ibid art 20(1).

28 ibid

29 ibid arts 19(1) and 20(2).

30 ibid art 20(2).

31 ibid art 19(2).

32 ibid art 19(4)(5).

33 ibid art 19(7).

34 Commission, (n 7) 12.

the provision in Article 20 of the RER on 'mutual agreements between courts and competent authorities regarding practical solutions for the examination that the examination of a person should take place in the premises of the court.[35]

10 To further examine the admissibility of the application of AI, it should be noted that although the RER is part of European international procedural law, the procedural elements outlined above are mainly standardised in legal and technical terms to facilitate judicial cooperation and the taking of evidence. Similarly to Regulation 1206/2001, the RER does not regulate fundamental procedural issues, such as the admissibility and the probative value of evidence and other rules on the taking of evidence, but leaves these to national procedural autonomy.[36] Indeed, the RER provides that the requesting court shall conduct the direct taking of evidence in accordance with its national law.[37] Thus, the RER follows the generally accepted rule that the rules of evidence are to be assessed according to *lex fori*, i.e., according to the procedural law of the court taking a particular procedural action.[38] The direct cross-border taking of evidence under *lex fori* contributes to the uniform treatment of evidence throughout the entire procedure conducted in one Member State, irrespective of the fact that certain evidence is taken abroad.[39] The opposite is the case with the indirect taking of evidence, when the requested court executes the request according to *lex fori*, i.e., according to its evidence-taking rules, because in this case that court undertakes a specific procedural action. But, subsidiarily it may also execute the request in accordance with the national law of the requesting court, if the latter has requested it and if such taking of evidence is neither contrary to the national law of the requested court nor entails major practical difficulties.[40]

11 Finally, it should be noted that in view of the challenges of justice in the period of the COVID-19 pandemic and in order to achieve the digital objectives in the field of justice, the European Commission adopted the Proposal for a Regulation of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation (hereinafter: Proposal on the digitalisation of judicial cooperation).[41] The aforementioned Proposal on the digitalisation of judicial cooperation proposes, *inter alia*, the use of videoconferencing for holding oral hearings in cross-border disputes in order to facilitate access to justice.[42] However, it is important to distinguish the scope of the Proposal on the digitalisation of judicial cooperation from the scope of the RER. The Proposal on the digitalisation of judicial cooperation provides for the introduction of videoconferencing for holding oral hearings when one of the parties to the proceedings is located in a Member State different from the one before whose court the proceeding is conducted.[43] Thus, it is only a question of facilitating the participation of the parties in cross-border proceedings via videoconference, but not about the taking of evidence, to which the provisions of the RER would continue to apply.[44]

C. The principle of immediacy vs videoconferencing systems in the cross-border taking of evidence.

12 In this section, we will consider the compatibility of the principle of immediacy with the use of videoconferencing systems in the direct cross-border taking of evidence by examining persons. It is a principle that has a long standing tradition across all European civil procedural law.[45] Indeed, as a civil procedure principle dealing with evidence-taking, the principle of immediacy imposes several requirements on the court. Among other things,

35 Ontanu, (n 24) 595.

36 Poretti, (n 19) 224.

37 Revised Evidence Regulation, art 19(8).

38 Franceso Parisi, Daniel Pi and Alice Guerra, "Access to Evidence in Private International Law" (2022) 23(1) Theoretical Inquiries in Law 14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964387> accessed 1 August 2022.

39 Đuro Vuković and Eduard Kunštek, *Međunarodno građansko postupovno pravo* (2nd edn, Zgombić&Partneri 2005) 188.

40 Revised Evidence Regulation, art 12(2)(3).

41 Commission, "Proposal for a Regulation of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation" COM/2021/759 final (hereinafter: Proposal on the digitalisation of judicial cooperation).

42 Xandra Kramer, "Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe" [2022] 56 *Revista General de Derecho Europeo* 5.

43 Commission (n 41) 27.

44 Kramer (n 42) 5.

45 European Law Institute and UNIDROIT (n 2) 114.

this principle requires the court understands the nature and content of evidence and to decide on its probative value.[46] There is no doubt that by introducing videoconferencing as a default form of direct evidence taking, the RER contributes significantly to strengthening the principle of orality and immediacy.[47] The court conducting proceedings in one Member State should no longer need to obtain information about a particular statement through the requested court of another Member State, considering that in practice, according to the previously mentioned statistics, indirect taking of evidence was the most widespread.[48] However, although it has been strengthened, the question arises of whether the principle of immediacy has been fully realised through videoconferencing. This question arises because videoconferencing as a technical solution still limits the direct observation of the court in terms of the immediate perception of the person testifying.[49]

13 In addition to the substantive and logical assessment of coherence, the realisation of the principle of immediacy allows the court to apply psychological criteria in assessing the probative value of statements. The court can pay attention to a respondent's gestures, the volume and tone of voice, as well as their relative persuasiveness in giving a statement, and thus it gets the opportunity to exercise the principle of free evaluation of evidence in its entirety.[50] The conducted research shows that the use of videoconferencing has an impact on the assessment of the credibility of statements.[51] Namely, the statements given by persons physically present in the courtroom are usually assessed by the court as more reliable and convincing than those made by videoconference.[52] A "digital barrier" in the form of a videoconference can lead to a wrong perception of the respondent's emotions, which can consequently have an impact on the establishment of facts by the court.[53]

14 The ELI/UNIDROIT Model European Rules of Civil Procedure suggest the use of videoconferencing in the cross-border taking of evidence in the EU as one of the possible options.[54] However, under the European Rules of Civil Procedure, the general position on the examination of witnesses or experts is that their oral statements are considered more reliable if those witnesses or experts are physically present in the courtroom when giving their statements.[55] ELI/UNIDROIT acknowledges that the use of videoconferencing contributes to the effectiveness and efficiency of the procedure. However, it is pointed out that the principle of immediacy is not fully achieved by the use of videoconferencing, as it is not equivalent to the physical presence of the respondent.[56] Therefore, it can be concluded that due to its shortcomings, the use of videoconferencing is a kind of substitute for physical contact between the court and the evidence.[57] In order to bridge the gap between physical and virtual presence in cross-border taking of evidence, and to fully realise the principle of immediacy, the next section considers some AI-based solutions that could possibly help to achieve this.

D. AI-based systems for assessing the credibility of statements.

15 In assessing the credibility of certain statements, AI is based on the application of machine learning such that the behaviour of respondents during their statements is compared to previously stored features of true or false statements collected

46 Siniša Triva and Mihajlo Dika, *Građansko parnično procesno pravo* (7th edn, Official Gazette 2004) 185.

47 Viktória Harsági, „Digital Technology and the Character of Civil Procedure" in Miklós Kengyel and Zoltán Nemessányi (eds), *Electronic Technology and Civil Procedure* (Springer 2012) 131.

48 See n 5.

49 Harsági (n 47) 131.

50 Triva and Dika (n 46) 186.

51 Alicia Bannon and Janna Adelstein, "The Impact of Video Proceedings on Fairness and Access to Justice in Court" (Brennan Center for Justice at New York University School of Law 2020) 6-7. <https://www.brennancenter.org/our-work/research-reports/impact-video-proceedings-fairness-and-access-justice-court> accessed 4 August 2022.

52 ibid

53 Amy-May Leach et al., "COVID-19 and the courtroom: how social and cognitive psychological processes might affect trials during a pandemic" (2021) 28(8) Psychology, Crime & Law 738.

54 European Law Institute and UNIDROIT (n 2) 171.

55 ibid 148.

56 ibid 161.

57 Georg E. Kodek, "Modern Communications and Information Technology and the Taking of Evidence" in Miklós Kengyel and Zoltán Nemessányi (eds), *Electronic Technology and Civil Procedure New Paths to Justice from Around the World* (Springer 2012) 274.

from respondents under controlled conditions.[58] According to previous research and the level of development, three basic techniques for assessing the credibility of respondents' statements can be distinguished: a) analysis of non-verbal behaviour, b) analysis of verbal behaviour, and c) analyses based on the brain imaging method (functional magnetic resonance imaging – fMRI).[59]

16 Analysis of non-verbal behaviour is usually based on the detection of false statements based on facial or eye movements.[60] Research shows that there is an interdependence between the expression of emotions and facial expressions, since facial expressions are neurologically controlled by two brain centres whose task is to control spontaneous and non-spontaneous facial movements.[61] In the case of true statements, emotions are spontaneous and consequently, facial expressions of the respondents are produced equally spontaneously.[62] However, if the respondent makes a false statement, both brain centres are activated and a neurological conflict occurs between spontaneous and non-spontaneous facial reactions, which are manifested in the form of micro expressions.[63] Furthermore, according to research, the eyes can also be a source for assessing the credibility of statements. Indeed, software has been developed that monitors eye tracking and blinking, as well as pupil dilation, and it uses these signs to assess the credibility of statements. According to some research results, it is reliable up to 90%.[64]

17 Analysis of verbal behaviour assesses the credibility of statements by measuring the respondent's voice stress level, which is higher in the case of deliberate deception, or even by linguistic analysis, which analyses the words spoken by the respondent and their frequency, which may imply a non-credible statement.[65] According to some research, linguistic analysis is reliable in deception detection in approximately 75% of cases.[66]

18 The European Union has also shown interest in non-verbal behaviourbased systems for assessing the credibility of statements. Namely, a virtual avatar was developed within the framework of the EU-funded iBorderCtrl project, which is based on the Automatic Deception Detection System (ADDS) whose purpose is to analyse the non-verbal behaviour of travellers.[67] The ADDS was tested in such a way that third-country nationals were questioned by an avatar via a web camera before arriving at the border crossing as part of the pre-registration process, in order to assess the credibility of their statements regarding the reasons for travelling.[68] The ADDS assessed the credibility of statements based on facial recognition technology and measurement of facial micro-expressions.[69] The accuracy of ADDS in detecting true statements was about 76%, while the reliability in detecting false statements was about 74%.[70]

19 Brain imaging-based analysis (fMRI) originated in the field of neuroscience. It was developed to detect misleading or deceptive statements based on blood flow in the brain, because it is believed that when a statement is false, parts of the brain are activated that are not normally active when the statement is true.[71]

20 In the context of this paper, systems that analyse both

58 M. U. Şen, V. Pérez-Rosas, B. Yanikoglu, M. Abouelenien, M. Burzo and R. Mihalcea, "Multimodal Deception Detection Using Real-Life Trial Data" (2020) 13(1) IEEE Transactions on Affective Computing 306 <https://ieeexplore.ieee.org/document/9165161/> accessed 4 August 2022

59 Tommaso Fornaciari and Massimo Poesio, "Automatic deception detection in Italian court cases" (2013) Artificial Intelligence and Law 306 <https://link.springer.com/article/10.1007/s10506-013-9140-4#citeas> accessed 5 August 2022

60 Bradshaw (n 1) 709.

61 Joan Pico, "The new challenges of evidence law in the fourth industrial revolution" in Koichi Miki (ed), *Technology, the global economy and other new challenges for civil justice* (Intersentia 2021) 486

62 ibid

63 ibid

64 Bradshaw (n 1) 709.

65 Fornaciari and Poesio (n 59) 307-308.

66 Fornaciari and Poesio (n 59) 308.

67 T. Krïgel, R. B. Schïtze and J. Stoklas, "Legal, ethical and social impact on the use of computational intelligence based systems for land border crossings" (2018) International Joint Conference on Neural Networks (IJCNN) 1 <https://ieeexplore.ieee.org/document/8489349> accessed 7 August 2022.

68 ibid 1-2.

69 Javier Sánchez-Monedero and Lina Dencik, "The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl" (2022) 25 (3) *Information, Communication & Society* 414 <https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1792530> accessed 7 August 2022

70 ibid 419.

71 Bradshaw (n 1) 709.

verbal and nonverbal behaviour are hypothetically considered for assessing the credibility of statements in the cross-border taking of evidence by videoconference. Indeed, for most systems, all that is needed is a web camera, a computer, a microphone, and an Internet connection,[72] i.e., essentially everything that is needed for taking evidence by videoconference, with the addition of automatic deception detection software.

E. The admissibility of using artificial intelligence in the assessment of the credibility of statements in the cross-border taking of evidence

21 The RER does not prescribe fundamental procedural elements for taking evidence, such as the admissibility and probative value of the evidence but leaves this to national procedural law.[73] However, it would be wrong to conclude that Member States are completely free with regard to the possible use of deception detection systems when taking evidence. Issues of admissibility of evidence are important to protect the fundamental rights of participants in the proceedings. Consequently, the admissibility of evidence can affect the effectiveness of cross-border judicial cooperation, which is closely related to the principle of mutual trust.[74]

22 Some Member States expressly regulate the inadmissibility of evidence by procedural law, alternatively this assessment of inadmissibility is developed through case law. Thus, for example, French law qualifies all evidence as inadmissible if obtained in an unfair manner.[75] French judges connect the unfairness of the evidence with the relevant provisions of the national Code of Civil Procedure, but also with the right to a fair trial guaranteed by the ECHR.[76] Moreover, if a decision involves an assessment of the behaviour of a particular person, French law does not allow judicial decisions to be based on the application of algorithms and automated processing of personal data.[77] According to Slovenian case law, the results of a polygraph as evidence in civil proceedings are considered inadmissible because the polygraph has elements of coercion, and it is up to the court to assess the reliability of an individual statement by applying the principle of free evaluation of evidence.[78] The situation is similar in Germany, where the results of the polygraph test are considered inadmissible evidence, even if the test was performed on a voluntary basis.[79]

23 Namely, it was previously said that the requesting court conducts the direct taking of evidence in accordance with the law of its Member State.[80] However, the central body or competent authority of the requested Member State is authorized to reject this request if, *inter alia*, it would be contrary to the fundamental principles of the law of requested Member State.[81] Therefore, the question arises whether the requested Member State would be authorized to reject the request for the taking of evidence with the application of a deception detection system, due to the contradiction with the fundamental principles of law of the requested Member State?

24 The answer to the question is not simple. However, in respecting national procedural peculiarities, the answer to the question could go in the negative direction. Namely, for direct taking of evidence by examining a person via videoconference, the court of the requested Member State can only provide technical support to the requesting court.[82] Furthermore, the direct taking of evidence by examining a person is always carried out on a voluntary basis, and the person testifying must be aware of the voluntariness of the testimony.[83] Therefore, it could be concluded that in the case of the application of the deception detection system by the requesting court, there would be no basis for the authority of the requested Member State to reject the request for the direct taking of evidence. Namely, the entire procedure is carried out before the court of the requesting Member State, which uses the

72 ibid

73 See n 33.

74 Župan (n 17) 473.

75 Vesna Rijavec and Tomaž Keresteš, „Restrictions on the Admissibility of Evidence“ in C.H. van Rhee and Alan Uzelac (eds), *Evidence in Contemporary Civil Procedure* (Intersentia 2017) 98.

76 ibid

77 Florence G'sell, „AI Judges“ in Larry A. DiMatteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence* (CUP 2022) 353.

78 Rijavec and Keresteš (n 75) 91-2.

79 ibid 92.

80 See n 37.

81 See n 33.

82 Revised Evidence Regulation, arts 19(6) and 20(2)

83 ibid, art 19(2)

deception detection system, while the requesting Member State only provides technical support in terms of computers, cameras, and microphones. Moreover, the examination of a person is carried out exclusively on a voluntary basis, and the person who needs to be heard is authorized to refuse to participate in the testimony. However, from the above it is still not possible to conclude that such a way of taking evidence would really be in accordance with the fundamental rights of the requesting Member State.

25 On the other hand, the situation regarding the issue of admissibility of evidence could be more challenging in the case of recognition and enforcement of judgements of one Member State in another Member State, if such a judgement originates from a procedure in which the deception detection system was applied. In that case, the Member States could, at the request of the interested party, refuse recognition and enforcement of the judgement due to conflict with public policy in the requested Member State, based on the Brussels Ibis Regulation[84]. Namely, the disparity of national procedural rules in the taking and evaluation of evidence *per se* is not a sufficient reason for establishing a violation of public policy.[85] However, the requested Member State may apply the public policy clause if recognition or enforcement of the judgement would violate rules considered essential in the legal order of the requested State or would constitute a violation of fundamental rights.[86] Fundamental rights are part of the general principles of law arising from the constitutions of the Member States and international treaties on the protection of human rights to which the Member States are parties.[87] Moreover, the Court of the European Union specifically indicates the importance of the ECHR and the right to a fair trial as a general principle of Community law.[88]

26 Considering the above and that the application of AI is considered for deception detection in the context of cross-border evidence collection based on the RER, the admissibility of the application of AI should be assessed against its compatibility with the right to a fair trial, which is guaranteed by the CFR and which Member States are obliged to respect when implementing EU law,[89] i.e., by the ECHR, to which all Member States are contracting parties.[90] Furthermore, with respect to personal data, it is established that any processing of personal data carried out in compliance with the RER must be compatible with the GDPR.[91] Therefore, in the next sections of the paper, the admissibility of the application of the deception detection system will be considered through the prism of the right to a fair trial and the GDPR provisions, and the compatibility of the system for assessing the credibility of statements with the draft AI Act will be considered as an additional contribution to this topic.

I. Right to a fair trial

27 It is known that the right to a fair trial (Article 6 of the ECHR, Article 47 of the CFR) consists of several elements. By analogy, the selected elements will be analysed in terms of the compatibility of the deception detection system with the right to a fair trial. Given that this paper analyses the possible application of a deception detection system in the cross-border taking of evidence, it is necessary to consider the views of the European Court of Human Rights (hereinafter: ECtHR) regarding the evidence itself. According to the case law of the ECtHR, the admissibility of evidence and the method of its assessment and probative value fall within the jurisdiction of national law and national courts.[92] However, this does not mean that national courts completely disregard the right to a fair trial with respect to the evidence-taking procedure. Indeed, the ECtHR assesses the fairness of the procedure as a whole, i.e., it assesses all aspects of the procedure, including the manner in which the evidence was

84 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) OJ L351/1 (hereinafter: Bruxelles I bis Regulation), arts 45(1)(a) and 46.

85 Stefano Dominelli, „Unjustified Interruption of the Taking Evidence by the Court of Origin as a Ground to Refuse CrossBorder Enforcement Under the Brussels I Rules" (2022) 1(2) The Italian Review of International and Comparative Law 403 <https://doi.org/10.1163/27725650-01020009> accessed 11 August 2022

86 ibid 403-4.

87 ibid 404.

88 ibid

89 Charter of Fundamental Rights of the European Union [2016] OJ C 202, art 51(1)

90 Council of Europe, "Chart of signatures and ratifications of Treaty 005" (2022) <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005> accessed 11 August 2022

91 Revised Evidence Regulation, art 30(1).

92 Päivi Hirvelä and Satu Heikkilä, *Right to a fair trial* (Intersentia 2021) 104. See also *García Ruiz v Spain* App no 30544/96 (ECtHR, 21 January 1999); *Tiemann v France and Germany* App no 47457/99 47458/99 (ECtHR, 27 April 2000)

taken.[93] It follows from the above that there is nothing to prevent the introduction of a deception detection system into national procedural systems. However, this still does not mean that the right to a fair trial would not be violated in terms of assessing the fairness of the entire procedure and compatibility with other elements of the right to a fair trial.

28 The first controversial reason in the application of the deception detection system is the possible violation of the right to access the court. Namely, the right of access to a court guarantees that everyone has the right to have their civil rights and obligations decided by an independent and impartial court.[94] Given that the deception detection system would also have a certain influence in the procedure, the right could be violated. The right to access the court guarantees a decision by the court in a certain dispute.[95] It should be considered that the decision-making process includes a whole series of procedural actions that precede the rendering of a judgment. Evaluation of evidence is also one of such actions, the purpose of which is to determine the facts to which the law is applied. Therefore, if the deception detection system were to be applied in the assessment of the credibility of statements, it would be uncertain whether the court truly independently decided on disputed facts and the criteria that it utilized.

29 The next question that arises is in which cases is it necessary to foresee the use of a deception detection system. If only persons heard by videoconferencing were subjected to a deception detection system, then the party whose proposed witness is heard by videoconferencing would be put in an unequal position. The testimony of that witness would be subjected to a stricter assessment regime compared to other witnesses who testify in court in person. Such treatment could be in conflict with the right to the procedural equality of arms, which requires that each party be given a reasonable opportunity to present its case under conditions that do not place the party at a substantial disadvantage compared to the opponent.[96] According to the case law of the ECtHR, a different approach in dealing with the examination of witnesses from the opposing parties may call into question the principle of equality of the parties and constitute a violation of the right to a fair trial.[97] The right to adversarial proceedings before the court is also connected with the principle of equality of arms. The adversarial principle guarantees the parties to discuss all relevant procedural material before the court.[98] Namely, the parties have the right to be informed and to state their opinion on all evidence or statements presented in order to influence the court's decision.[99] Although optional for the court, the results of the deception detection system would certainly constitute a body of procedural material, and the parties should be able to discuss the content of these results. However, the expert knowledge of the parties, as well as judges and lawyers, about the technology of deception detection systems appears as a potential difficult problem to overcome. As a complex technology that is difficult to understand for most citizens, it could represent an obstacle in the discussion of the obtained results, and thus in the actual exercise of the right to adversarial proceedings.

30 There is also a danger that the application of the deception detection system will become a routine for the judge who does not independently assess the results obtained in relation to statement credibility, but automatically accepts them. This would constitute a possible violation of the right to an independent and impartial court and the right to a reasoned court decision. Namely, the court is obliged to properly consider the submissions, arguments and evidence presented by the parties, without prejudice to their assessment of whether they are material to its decision.[100] Therefore, it is the duty of the judge to examine each piece of evidence and reach a conclusion on its credibility and relevance. Furthermore, the court is obliged to justify its actions through the explanation of its decision.[101] Therefore, the court would have additional obligations to explain how it evaluated the obtained results of the deception detection system and why it accepted or did not accept the results of the deception detection system.

31 In the first part of the paper, it was mentioned that pursuant to the RER, the direct cross-border production of evidence is carried out on a voluntary

93 *Elsholz v Germany* App no 25735/94 (ECtHR, 13 July 2000)

94 Alan Uzelac, „Pravo na pravično suđenje u građanskim predmetima: Nova praksa Europskoga suda za ljudska prava i njen utjecaj na hrvatsko pravo i praksu" (2010) 60(1) Zbornik Pravnog fakulteta u Zagrebu 107.

95 *Lupeni Greek Catholic Parish and others v Romania* App no 76943/11 (ECtHR, 29 November 2016)

96 *Užukauskas v Lithuania* App no 16965/04 (ECtHR, 6 July 2010)

97 *Ankerl v Switzerland* App no 17748/91 (ECtHR, 23 October 1996)

98 Uzelac (n 94) 109.

99 *Ruiz-Mateos v Spain* App no 12952/87 (ECtHR, 23 June 1993)

100 *Carmel Saliba v Malta* App no 24221/13 (ECtHR, 29 November 2016)

101 *Suominen v Finland* App no 37801/97 (ECtHR, 1 July 2003)

basis. Accordingly, the application of deception detection systems should also rest on the voluntary consent of the person testifying. However, the question arises as to what happens if the witness is willing to testify, but without applying a deception detection system. Indeed, the court could prejudge the unreliability of an individual witness if he or she refuses to use the deception detection system, which could lead to subjective bias on the part of the court. According to the case law of the ECtHR, impartiality is determined using a subjective test that takes into account personal beliefs and behaviour of an individual judge, i.e., whether the judge had personal prejudice or bias in a particular case.[102] Therefore, if a witness refuses to be assessed by the deception detection system, this could establish unfounded subjective bias on the part of the judge, which could ultimately impact the dispute resolution process between the parties and violate the right to a fair trial. Also, the introduction of the deception detection system into the procedural law could raise doubts about the objective impartiality of the court as a judicial body, as it would call into question the public's trust in the courts, whose existence is necessary in a democratic society.[103] The aforementioned could contribute to the collapse of the mutual trust between citizens and the state, because the AI, through its application in court proceedings, would encroach on the very essence of the relationship between citizens and the state.[104]

32 The next question that arises is how to qualify the legal status of the deception detection system in procedural law. Is this system an expert *sui generis,* or an auxiliary tool of the court? It should be obvious that the deception detection system cannot be an expert, because experts are natural persons.[105] However, if it is taken into account that the deception detection system, based on its specific technical characteristics, makes an assessment of the credibility of statements, then it can be concluded that the deception detection system would be an auxiliary tool of the court for risk assessment, which, like an expert, observes and renders an opinion on the facts that are essential for assessing the veracity of allegations that are the subject of evidentiary proceedings.[106] Moreover, the parties always have the right to rely on the results and opinions of experts and even to raise the objection that the expert is biased. But how can you object to the deception detection system, or will the parties be informed of the individual statement credibility assessment results? With regard to the findings and opinions of experts that relate to a technical field that is not within the scope of knowledge of judges, the ECtHR took the position that such opinions are likely to have a dominant influence on the judge's evaluation of the facts.[107] Therefore, it would be necessary to give the parties an opportunity to look back at the results of the deception detection system, which would serve as an auxiliary tool of the court for risk assessment. Moreover, the influence on the judge would certainly be significant, and it would be necessary for the judge to discuss with the parties the relevance of the results of the deception detection system. The same is stated in the ELI/UNIDROIT Rules of European Civil Procedure. Namely, the ELI/UNIDROIT Rules allow the use of AI to the extent that it is compatible with the right to be heard. However, the Rules require that the use of AI be transparent, in such a way that the parties know that AI is being used and that they can discuss the nature, quality and conclusions that can be drawn from the application of AI.[108]

33 Furthermore, there is a real danger that the system could be biased against certain social groups based on gender, ethnicity or cultural affiliation. Therefore, the representativeness and quality of the stored data is critical to ensure that it faithfully represents all social groups.[109] For example, people of different genders may have different facial expressions, gestures or verbal expressions, while patterns of one gender predominate in the stored templates of the deception detection system.[110] All of this affects the reliability of the results obtained and the overall assessment of whether the procedure was fair, respecting other rights guaranteed by the ECHR. In addition, low-quality IT equipment or Internet connection may negatively affect the image or sound received during the cross-border taking of evidence, which may lead to unreliable results of the deception detection system. Through the ECtHR´s case law, bad acoustics, and even the image, can be reasons that may lead to a violation of the right to

102 *Micallef v Malta* App no 17056/06 (ECtHR, 15 October 2009)

103 *Wettstein v Switzerland* App no 33958/96 (ECtHR, 21 December 2000)

104 European Law Institute and UNIDROIT (n 2) 23.

105 Triva and Dika (n 46) 527.

106 ibid 526.

107 *Mantovanelli v France* App no 21497/93 (ECtHR, 18 March 1997)

108 European Law Institute and UNIDROIT (n 2) 23.

109 Jo Ann Oravec, „The emergence of "truth machines"?: Artifcial intelligence approaches to lie detection" (2022) 24(6) *Ethics and Information Technology* 6. <https://doi.org/10.1007/s10676-022-09621-6> accessed 11 August 2022

110 Bradshaw (n 1) 717.

a fair trial.[111]

II. General Data Protection Regulation (GDPR)

34 As mentioned above, deception detection systems can analyse a number of behavioural factors, including facial micro-expressions, eye tracking and voice cues. Given that these factors are evaluated using a range of technical tools, including video cameras, microphones and AI-based software, this could initially lead to a wrong impression that this is about biometric data processing. However, in the context of the GDPR, the application of the deception detection system would not fall under a stricter regime of processing special categories of data provided for in Article 9 of the GDPR.[112] Namely, the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".[113] As the purpose and function of a deception detection system is to determine the credibility of a particular statement, and not the identity of the respondent, it is obvious that the application of such systems does not fall within the scope of the stricter regime for the processing of special categories of data. Indeed, deception detection systems do not perform biometric comparisons, but compare individual factors, such as facial microexpressions, with factors of the same type that are crucial for determining the credibility of statements.[114]

35 However, the processing of personal data,[115] which is a broader term than biometric data, could fall within the context of deception detection systems under the provisions on automated individual decision-making, including profiling.[116] According to Article 4(4) of the GDPR, profiling means:

> "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

36 In accordance with the provisions of the GDPR, the data subject has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[117] Put simply, the aim of the said provision is to prevent decisions related to individuals from being made by machines whose content is not subject to human judgement.[118] The provision prohibiting automated data processing, including profiling, applies regardless of whether the final decision produces positive or negative effects, until its content is decided by a human being.[119] In relation to the prohibition of automated data processing and profiling, the GDPR prescribes certain exceptions. The aforementioned will still be permitted, *inter alia*, if it is authorised by European Union or Member State law to which the controller is subject and which also lays down appropriate measures to protect the rights and freedoms as well as legitimate interests of the data subject; or if the decision is based on the express consent of the respondent.[120]

37 There is no doubt that deception detection systems use personal data from which they extract certain

111 *Stanford v United Kingdom* App no 16757/90 (ECtHR, 23 February 1994)

112 Art 9(1) of the GDPR expressly prohibits, *inter alia*, the processing of biometric data, unless there exists one of the legal bases listed in art 9(2) of the GDPR.

113 GDPR, art 4(14)

114 Els J. Kindt, "Biometric data processing: Is the legislator keeping up or just keeping up appearances?" in Gloria González, Rosamunde Van Brakel, and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Edward Elgar Publishing 2022) 385.

115 Pursuant to art 4(1) of the GDPR, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

116 Keeley Crockett, Sean Goltz and Matt Garratt, "GDPR Impact on Computational Intelligence Research" (2018) International Joint Conference on Neural Networks (IJCNN) 4.

117 GDPR, art 22(1)

118 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 180-181.

119 ibid 181-182.

120 GDPR, art 22(2)

factors based on which they analyse the behaviour of the person giving the statement, but also predict his or her reliability. Therefore, it is clear that, as prescribed by the GDPR, the operations of the deception detection system can theoretically be subsumed under profiling. In the context of this paper, this would refer to the case when the judge taking evidence in cross-border matters by examining a person would independently evaluate neither the results of the deception detection system, nor the entire statement of the respondent, but would base his or her decision solely on the obtained results without the possibility of influence.[121] Of course, with the fulfilment of one of the previously mentioned conditions that exceptionally allow the application of automated data processing systems. This consideration is only theoretical since in practical application it is incompatible with the right to a fair trial. Namely, if the judge really had to accept the results of the deception detection system without his or her decisive influence, then the system would become the judge. Therefore, it should be concluded that if the final decision on the credibility of the statement is made independently by the judge, regardless of the results of the deception detection system, then we would not deal with automated individual decision-making, i.e., profiling, after all.[122]

III. Artificial Intelligence Act Proposal

38 Considerations on the compliance of the deception detection system with the AI Act proposal follow from previous GDPR-related considerations. Namely, among other proposed solutions, the AI Act sets out the transparency requirements regarding emotion recognition systems[123] that use biometric data and imposes an obligation that the respondent shall be informed of his or her interaction with such a system.[124] Under the AI Act Proposal, deception detection systems could fall under the definition for emotion recognition systems as long as biometric data is not specified as a basis for emotion recognition[125]. Given that the AI Act takes over the definition of biometric data from the GDPR, it follows that deception detection systems would still not be considered emotion recognition systems.[126]

39 However, since the use of AI-based deception detection systems is considered from the aspect of potential use in cross-border evidence taking, the AI Act still requires scrupulous handling. Namely, all AI systems intended to assist judicial bodies in researching and interpreting facts and law and in applying law to a specific set of facts are considered high-risk systems.[127] Given that deception detection systems, as an auxiliary tool of the court, participate in research and interpretation of facts, because through the analysis of respondent behaviour they assess statement credibility, it is obvious that such systems would be considered high-risk in the context of the AI Act. However, the classification of an AI system in the judiciary as high-risk does not necessarily mean permission to use such systems.[128] Namely, according to clarifications of the AI Act, the use of high-risk systems should only be possible if it complies with the CFR and secondary law of the European Union and national laws of the Member States.[129] From the above, it should be clear that a possible application of a deception detection system in evidence taking, in addition to compliance with the CFR, would also require standardisation in national procedural law. The use of this system is directly related to the basic procedural elements related to the assessment of the probative value. As already mentioned above, the RER is restrained in this direction and leaves itsubject to national law.[130]

40 Given that AI systems intended for use in the judiciary are classified as high-risk, the AI Act sets more rigorous requirements for such systems. Acknowledging that deception detection systems, using machine learning, compare signs that point to a non-credible statement with signs from a stored data set, the data quality requirement is important

121 Keeley Crockett, Sean Goltz and Matt Garratt (n 116) 4.

122 *Arg a contrario.*

123 Pursuant to art 3(34) of the AI Act Proposal, emotion recognition system means "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data".

124 Jan Czarnocki, "Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?" in: Brömme, A., Busch, C., Damer, N., Dantcheva, A., Gomez-Barrero, M., Raja, K., Rathgeb, C., Sequeira, A. & Uhl, A. (eds), *BIOSIG 2021 - Proceedings of the 20th International Conference of the Biometrics Special Interest Group* (Gesellschaft für Informatik e.V. 2021) 182.

125 See n 123.

126 Czarnocki (n 124) 182.

127 Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" (2021) 22(4) Computer Law Review International 102 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852> accessed 12 August 2022. See also art 6(3) of the AI Act and Anex III (8)(a) of the AI Act.

128 AI Act, recital 41.

129 ibid

130 See n 36.

in this context. Namely, the AI Act requires that the data sets meet the data quality criterion in such a way that they are relevant, representative, error-free and complete.[131] It is therefore necessary to ensure that the data stored in the deception detection system are regularly refreshed, with a complete and representative sample in terms of age, gender, race and other factors, in order to produce accurate results. Furthermore, *inter alia*, the AI Act requires human oversight of high-traffic AI systems.[132] The purpose of human oversight is to ensure that AI systems are subject to human control in order to reduce risks related to fundamental rights, health and safety.[133] Pursuant to the AI Act, human oversight requires a series of measures that enable users to understand the capabilities of the AI system, to interpret the results correctly, to stop, ignore or change the results at any time, and to intervene in the operation of the system.[134] Although the possibility of altering the results is reasonable and justified with the aim of protecting fundamental rights, attention should be paid to an interesting research study. Namely, the research was conducted under controlled conditions in order to determine whether the automatic deception detection system achieves greater accuracy in hybrid form, i.e., by the assessment of a judge who can reject the obtained results or adjust them within certain limits.[135] The research showed that human influence on the obtained results impairs their reliability, i.e., that judges are more inclined to classify answers as true even though they are not.[136] Therefore, based on the conducted research, the deception detection system proved to be more reliable than humans.[137]

41 In terms of human oversight, the concept of "automation bias" is interesting, which could also be a significant risk in the application of deception detection systems in cross-border evidence taking.[138] Namely, "automation bias" towards the AI Act is defined as "the tendency of involuntarily relying or over-relying on the output produced by a high-risk AI system (...), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons."[139] Accordingly, the risk for judges in the application of the AI-based deception detection system consists in the risk of routine application of such systems. Over-reliance and the uncritical acceptance of the results would not be compatible with the right to a fair trial. In that case, AI would become the indirect judge, while the judge would be only a formal decision maker, whose decisions would be made on the basis of mechanical downloads of the deception detection system results.

F. Concluding remarks

42 The introduction of the direct cross-border taking of evidence by examining persons via videoconference will, as the primary method, undoubtedly contribute to the realisation of the right to access to justice. However, although the principles of orality and immediacy have been significantly strengthened, there is still room for strengthening the latter. The presented research shows that AI-based deception detection systems are nevertheless more accurate in terms of assessing the credibility of statements than the average person. Therefore, the research question from the introductory part of the paper should be answered in such a way that there is the potential for the application of a deception detection system in the cross-border taking of evidence. On the other hand, there is no shortage of counterarguments regarding the admissibility. Namely, open research questions within the framework of respect for the right to a fair trial still point to reticence about the application of the deception detection systems in civil proceedings. Although, according to research, the accuracy of deception detection systems is higher than human, the risks associated with the application of such systems are far greater. Unconditional commitment to fundamental rights, an essential component of which is the right to a fair trial, contributes to citizens' trust in the courts and strengthening their legitimacy. Also, if in the future the introduction of these systems into the judiciary were to be considered more seriously, then coherence in the legislative approach of the Member States is necessary. A unique approach in standardizing the use of AI in cross-border taking of evidence contributes to the preservation and strengthening of cross-border judicial cooperation and prevents the violation of mutual trust between Member States. It is also necessary to strengthen the digital competences of legal experts so that they can

131 Veale and Zuiderveen Borgesius (n 127) 103.

132 ibid

133 ibid

134 AI Act, art 14(4)

135 Bennett Kleinberg and Bruno Verschuere, "How humans impair automated deception detection performance" (2021) 213 *Acta Psychologica* 1-8 <https://www.sciencedirect.com/science/article/pii/S0001691820305746> accessed 28 August 2022.

136 ibid

137 ibid

138 AI Act, art 14(4)(b).

139 ibid

adequately understand and explain the work and effects of AI-based systems to parties. This mainly applies to the work of judges, for whom it is of crucial importance to understand the work of the AI and to resist the automation.

Note: The research reflected in this article was financed by the Young Researchers' Career Development Project – Training New Doctoral Students, funded by the Croatian Science Foundation.