ECLIC 7 - SPECIAL ISSUE

EU AND COMPARATIVE LAW
ISSUES AND CHALLENGES SERIES

International Scientific Conference
on International, EU and
Comparative Law Issues

"Law in the Age of Modern Technologies"

SERIES EDITORS:
Tunjica Petrašević, Dunja Duić

GUEST EDITORS:
Katarina Trimmings
Francesca C. Villata
Mirela Župan

GUEST EXECUTIVE EDITOR:
Jura Golub

CONFERENCE BOOK
OF PROCEEDINGS

DIGITAL IN LAW

JOSIP JURAJ STROSSMAYER UNIVERSITY OF OSIJEK

PRAVOS

Co-funded by the
Erasmus+ Programme
of the European Union

UNIVERSITÀ DEGLI STUDI
DI MILANO
DIPARTIMENTO DI
STUDI INTERNAZIONALI,
GIURIDICI E STORICO-POLITICI

1495 UNIVERSITY OF ABERDEEN

srce
University of Zagreb
University Computing Centre

EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES
(ECLIC 7 – SPECIAL ISSUE)
ISSN (Online): 2459-9425

Publishers:
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek

This publication is co-funded by the Erasmus+ Programme of the European Union.

UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC 7 – SPECIAL ISSUE)

International Scientific Conference on International, EU and Comparative Law Issues

"Law in the Age of Modern Technologies"

Series Editors:
Tunjica Petrašević, Dunja Duić

Guest Editors:
Katarina Trimmings, Francesca C. Villata, Mirela Župan

Guest Executive Editor:
Jura Golub

CONFERENCE BOOK OF PROCEEDINGS

In Milan, 10 February 2023

Co-funded by the Erasmus+ Programme of the European Union

Publisher
Josip Juraj Strossmayer University of Osijek
Faculty of Law Osijek

For the Publisher
Tunjica Petrašević, PhD, Full Professor
Dunja Duić, PhD, Associate Professor

ISBN 978-953-8109-56-0

International Scientific Conference on International, EU and Comparative Law Issues

"Law in the Age of Modern Technologies"

TABLE OF CONTENT

FOREWORD

The volume before you represents one of the results of a collaboration established by a consortium of universities of Aberdeen, Milan, Osijek, and University of Zagreb University Computing Centre, within the framework of the Time to Become Digital in Law (DIGinLaw) project. The project was carried out from 1 April 2021 to 30 September 2023, and was fully funded by the European Union under the Erasmus+ programme.

The lead idea of this project was to turn something negative, which Covid-19 was, into an advantage. The valuable experience of teaching in a digital environment, which we were practically forced to pursue, should not remain in our memory for the moments of fear and infirmity. On the contrary, it was a historical moment when the ability of mankind to adapt to new and unpredictable situations has proven. Today it is crystal clear that a radical turn towards digital transformation entered each pore of the human society.

Our consortium has taken up pioneering steps in the field of law. Before this project, our collaboration mainly focused on joint research. Here we stepped out of those boundaries and decided to put ourselves in a new role: as true e-teachers have been trained, we struggled with methodology, didactics, and many digital tools; and we fought with adopting a perspective based on the central role of the student instead of the teacher. But, we as a team encouraged the development and improvement of digital literacy and digital competences of our students, indispensable for the functioning on the labour market of our time. Education that results in a so-called T-shaped lawyer not only prepares employees for this digital market, but also changes the attitude towards the development of the 21st century skills in general. We are happy to be on board of the HE of modern times. A particular value of this project is that at its end it has produced a number of MOOCS in the area of digitalization in law.

However, also within this project consortium, team members engaged with significant research activities. One of the aims of the project was to establish a pool of experts engaged in research in various aspect of digitalization affecting our daily lives. Researchers and experts met in Milan on 10 February 2023, at the International Scientific Conference on International, EU and Comparative Law Issues "Law in the Age of Modern Technologies", to present, network and discuss their research results. Papers written by the consortium team members were collected, made subject to a double-blind peer review and are presented here to the public. The dissemination of thorough research on this topic, which has become a matter

of the moment we live in, should be wide-ranging. Our vision for HE is based on inclusive and open resources for study and research, thus all of our results are available online.

It is an obligation of academics from all disciplines, from STEM to social sciences and arts and humanities, to contribute to a strategically planed, well thought through and fairly balanced regime of European digital future. Milestones achieved by this project are available on the project website.[1] Credit goes to each and every team member of the universities of Aberdeen, Milan, Osijek, and University of Zagreb University Computing Centre, as a backbone of this consortium. This volume speaks of their commitment, determination, persistence and openness to the new.

Katarina Trimmings, PhD, Professor
Francesca C. Villata, PhD, Full Professor
Mirela Župan, PhD, Full Professor

[1] Time to Become Digital in Law, [https://www.pravos.unios.hr/diginlaw/].

Topic 1

Digitalization of Law

UDK 341.4:004.7]:342.7
Original scientific paper

DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL PROCEEDINGS AND HUMAN RIGHTS CHALLENGES*

Chiara Ragni, PhD, Full Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
chiara.ragni@unimi.it

ABSTRACT

Digital technologies offer great opportunities in every field of life, including in criminal proceedings, where gathering evidence using digital or computer devices is an important contribution to the investigation of crimes, especially at the international level. Digital evidence is particularly important in the prosecution of international crimes due both to their complexity and to its ability to overcome hurdles that international judges must overcome when fact-finding relates to conduct that occurred far from the seat of the court. While the of digital evidence is increasing, however, questions have arisen concerning both its admissibility and of its reliability, as the jurisprudence of the International Criminal Court (ICC) and other international criminal tribunals makes clear. The use of digital evidence may also raise concerns for the respect of due process standards and the right to private life. In the absence of specific international legal rules that deal with the matter, the purpose of this contribution is to identify the most pressing issues through an examination of the case law of international tribunals and to infer potential solutions and best practices to consider in developing international human rights based procedural standards.

Keywords: *digital evidence; international criminal proceedings; international crimes; law of evidence; admissibility; reliability; human rights standards; right to private life; right to a fair trial*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

In recent decades, criminal investigators and judges have increasingly relied on digital technologies as a means of supporting fact-finding in relation to the commission of crimes, both in international and in domestic proceedings. In the international context, the availability of a broad range of digital tools, like video recordings, intercepted communications, open-source on-line information, aerial drone footage, social media content and geo-referenced field documentation has opened up broad opportunities to strengthen investigations of grave human rights abuses.[1]

The use of digital technologies in the prosecution of international crimes has allowed international criminal tribunals to overcome some of the hurdles they must face due to their distance (both geographical and temporal) from crime scenes and their dependence upon the cooperation of domestic authorities. In most cases, the difficulty of collecting some evidence, like witnesses' testimonies, for example, is even exacerbated by security reasons, especially in the contexts of political disorder or of armed conflict – contexts in which most international crimes are committed. Modern technologies and devices may help fill evidentiary gaps,[2] despite the fact that Tribunals must continue to rely on the cooperation not only of states but also of private entities, the activities of which provide them with large amounts of data.

The use of video and photographs as evidence in international legal proceedings is not new. It dates back to the Nuremberg trial, when live footage of the final days of World War II was shown in the courtroom and had a significant impact on the judges' assessment of the facts. As new technologies have developed, both in the field of forensic medicine and in the collection and storage of data and metadata, their importance in international criminal proceedings has grown, as we see from the case law of both the *ad hoc* International Criminal Tribunals[3] and, subsequently, of the International Criminal Court (ICC), both of which rely on ever more sophisticated tools.[4]

---

1 Land, M.; Aronson, J. (eds.), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018, spec. p. 125 ff.

2 Harmon, M.B., *Prosecuting Massive Crimes with Primitive Tools: Three Difficulties Encountered by Prosecutors in International Criminal Proceedings*, Journal of International Criminal Justice, Vol. 2, No. 2, 2004, pp. 403–426.

3 As to the ICTY, see for example *Prosecutor v Tolimir*, Case No. IT-05-88/2-T, Judgment, 12 December 2012, as regards the use of DNA analysis for the identification of the "Srebrenica-related missing" (*ibid.*, para 49 ff.) and of intercepted communications and aerial imagery (para 63 ff.) as evidence. For the ICTR, cf. *Prosecutor v Bagosora*, Case No. ICTR-98-41-T, Trial Judgment and Appeals Judgment, 8 December 2008 and 14 December 2011, respectively paras 2029-2031, 460, where the judges based on video footage their findings on the role of the defendant as the Rwandan Minister of Defence.

4 Freeman, L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal, Vol. 41, No. 2, 2018, pp. 283-336.

Although the potential of digital evidence and methods to assist in the prosecution of international crimes is undeniable, they also raise significant issues of both admissibility and reliability. As to the former, problems of admissibility may arise, for example, in the event data were collected in violation of privacy rights, which are protected by human rights legislation. As to the latter, one need only consider data posted on social media to perceive the concrete risks that they will be quickly removed before they can be preserved by investigators, or that they may represent fake or inaccurate information.

In light of these premises, then, the aim of the paper is to: i) examine the case law of International criminal tribunals, with a focus on the ICC, in order to identify cases in which the judges based their findings – at least in part – on digital evidence;[5] ii) identify the most problematic issues concerning the admissibility and reliability of this kind of evidence in light of the Rules of Procedure and Evidence (RPE) of International criminal tribunals and especially of the ICC; iii) investigate, with regard to the question of admissibility, how the international criminal tribunals have balanced the probative value of digital evidence with the respect of human rights.

2. THE INCREASING USE OF DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL PROCEEDINGS AND ITS ADVANTAGES

The jurisprudence of the international criminal tribunals reveals that, especially in recent years, they are increasingly using digital technologies for fact-finding purposes. As anticipated in the premise, in fact, digital evidence in international criminal proceedings has allowed the tribunals to address some of the problems that the prosecution of international crimes generally entails. In addition to the obstacles to collecting evidence mentioned above, digital tools are also well-tailored for addressing the specific features of international crimes. The complexity of such crimes due to the fact that they are not limited to a single act, but occur

[5] Even if there is no legal definition of digital evidence, it may be assumed that the term includes "any data [of value to an investigation] resulting from the output of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using any electronic device". European Commission, *European Data Informatics Exchange Framework for Courts and Evidence*, European Evidence Project, available online at [www.cordis.europa.eu/project/id/608185/reporting/de], Accessed 12 January 2022. Digital, or electronic, evidence has also been described by scholars dealing with the matter as "any probative material stored or transmitted in digital form, … which can be used in legal proceedings before a court in order to prove a fact according to the required standard of proof". For this definition, see Roscini, M., *Digital Evidence as a Means of Proof before the International Court of Justice*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 541-554.

as a part of a greater course of conduct and require proof of contextual as well as specific elements.[6]

In such cases, aerial and satellite images and video footage may be fundamental for demonstrating the existence of mass and grave destruction or killings, the movement of people or troops, and devastated areas. For example, the International Criminal Tribunal for the Former Yugoslavia (ICTY) made recourse, in the *Tolimir* case, to satellite imagery provided to the Prosecutor by the US military to prove the presence of gravesites and reburial activities, buildings and vehicles, large groups of prisoners, and bodies at particular locations. In *Krstić* aerial images were used for proving the mass and grave killings committed in Srebrenica.[7]

Examples of the use of satellite images as evidence of facts may be also found in the practice of the ICC. In the *Darfur* cases, for example, the Prosecutor made extensive reference to the report of the Commission of Inquiry, designated to ascertain the facts as they occurred during the Government's violent campaign against the rebels. The report, in turn, mostly relied on satellite images provided by human-rights organisations, which used them to detect the destruction and burning of villages, and the movement of refugees.[8] In the *Al Mahdi* case, the Prosecutor presented a significant amount of open source evidence, including satellite images found on Google Earth.[9] Although, as discussed below, the use of this kind of image as evidence may pose issues of reliability, their introduction into the proceeding reveals the pervasiveness internet and digital tools have reached even in the

---

6 On the advantages of digital evidence in prosecuting international crimes see Freeman, L., *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in: Dubberley, S.; Koenig, A.; Murray, D. (eds.), Digital Witness - Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67.

7 "Aerial photographs, taken on 17 July 1995, of an area around the Branjevo Military Farm, show a large number of bodies lying in the field near the farm, as well as traces of the excavator that collected the bodies from the field". The executions in Kozluk must have occurred between 14 July and 17 July 1995, given that aerial images show the mass grave in the Kozluk area was created prior to 17 July 1995 and the prisoners were not transported to the zone of responsibility of the Zvornik Brigade until 14 July 1995". *Prosecutor v Radislav Krstic*, Case No. IT-98-33, Judgement, 2 August 2001, respectively paras. 237 and 253.

8 International Commission of Inquiry on Darfur, *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General*, 2005, paras. 183 and 301, [https://www.legal-tools.org/doc/1480de/pdf/], Accessed 12 January 2023. On the use of satellite imagery as evidence in the jurisprudence of the ICC see Sandalinas, J., *Satellite Imagery and its use as Evidence in the Proceedings of the International Criminal Court*, Zeitschrift Für Luft-Und Weltraumrecht: Vierteljahresschrift Des Instituts Für Luft- Und Weltraumrecht Der Universität Köln, Vol. 64, No. 4, 2015, pp. 666-675.

9 *Prosecutor v Al Mahdi*, Case No. ICC-01/12-01/15-171, Decision on the confirmation of charges against Ahmad Al Faqi Al Mahdi, 24 March 2015. For a comment see Freeman, L., *Prosecuting…*, *op. cit.*, note 6, p. 316 ss.

forensic context. This pattern continues in the use of modern technologies, and, in particular, of aerial and satellite images of bodies on the streets of Ukrainian cities, to document the killing of civilians by the Russian army and, therefore, to indicate the commission of war crimes.

Digital evidence has also proven relevant for demonstrating a person's involvement in a criminal conspiracy or in planning, ordering and directing the perpetration of international crimes, the commission of which is generally the result of a precise policy or of criminal design. Intercepted communications are important for this purpose, and have been used extensively by all the International criminal tribunals.

In *Blagojević* and *Jokić*, intercepted communications were presented by the Prosecutor of the ICTY as evidence of the "communications between officers and soldiers of the VRS Main Staff, Drina Corps and subordinate brigades during the weeks before, during and after the fall of Srebrenica… Indeed, taken individually, certain intercepts provide direct evidence of the accused's knowledge of and/or participation in the forced removal of civilian Muslims from Srebrenica and the subsequent massacre of Srebrenica's Muslim men. Perhaps more importantly, as a whole, the intercept evidence tells the story of the VRS military participation in the attack on Srebrenica and the events that follow, and forms an important part of the mosaic of evidence to be introduced by the Prosecution".[10] In *Popović*, intercepted communications were used to demonstrate the chain of command and provided a narrative of the VRS attack on Srebrenica and the events that followed.[11]

Telecommunications evidence, including call data records and cell site information, were presented before the Special Tribunal of Lebanon (STL), the sole international court to have jurisdiction over the crime of terrorism, to prove the preparatory acts leading up to the terrorist attack which killed the Prime Minister of Lebanon, Rafiq Hariri on 14 February 2005. In *Ayyash et a.*, call data records served to prove both communications among the accused persons and that the network mobiles were engaged in Mr Hariri's surveillance and assassination.[12]

---

10 *Prosecutor v Blagojević and Jokić*, Case No. IT-02-60-T, Decision on the admission into evidence of intercept-related materials, 18 December 2003, para. 4.

11 *Prosecutor v Popović et al*, Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, 7 December 2007.

12 *Prosecutor v Ayyash et al*, Case No. STL-11-01, Decision on Motions for the Admission of the Call sequence tables related to the five colour-coded mobile telephone groups and networks call sequence tables, 31 October 2016. See Fremuth, M., *Prosecutor v Ayyash et al (Special Trib. Leb.)*, International Legal Materials, Vol. 60, No. 3, 2021, pp. 357-447.

The ICC has also relied on intercepted communications. In *Ongwen*, the Prosecutor presented Lord's Resistance Army (LRA) radio communications intercepted by Ugandan security agencies to the Chamber as evidence. In particular, it submitted to the Court a logbook summary of the information intercepted, which had been prepared by interceptors at the end of a series of interceptions, and which aimed to transcribe and summarize in English the content of the communications (which were predominantly in Acholi or Luo, two local dialects). The interceptors gave their logbook entries to their commanders, who transmitted the intercepted communications to Kampala to inform the Uganda People's Defence Force's broader military operations. All the completed recordings and logbooks were securely stored, either at the sites of interception or in Kampala.[13] What the Prosecutor submitted to the Chamber was the product of both a selection made by the Uganda governmental authorities when they transmitted the records and notes taken by interceptors and of a process of "enhancement" of audio recordings.[14] To overcome doubts and criticisms that accompanied the submission of intercepted communications, a fundamental role was played by the so-called 'intercept witnesses'—witnesses able to discuss the interception's operations as well as specific intercepted communications. The witnesses were called by the Prosecutor to testify before the Court with the aim, first, of identifying the speakers and confirming the correspondence of the audios with the transcripts, on, second, of explaining the methodology used to enhance the audio for the purpose of criminal proceedings. Leaving for aside all these issues, which will be better discussed here below, it is worth noting that intercepted communications were used as evidence of Ongwen's rank as a brigade commander and of his "interactions, in particular of the LRA's radio communication network, during which intentions to harm civilians on account of their perceived association with the Government of Uganda were discussed. In addition, the Chamber finds support for this conclusion in its findings in relation to Dominic Ongwen's involvement in the four attacks relevant to the charges."[15]

Notwithstanding the increasing importance of digital evidence in international criminal proceeding, defendants have often challenged its admissibility and reli-

---

13 *Prosecutor v Dominic Ongwen*, Case No. ICC-02/04-01/15, Judgment, 4 February 2021, para. 614 ff.

14 As we will see in greater detail (*infra*, sections 3-4), the procedure followed for this kind of evidence raised several concerns as regards its reliability, that were brought by the Defence to the attention of the Court. See in this regard the analysis made by Marchesi, D., *Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC*, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940.

15 *Ongwen*, *op. cit.*, note 13, paras. 1146-1147. For more examples see Freeman, L.; Vazquez Llorente, R., *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188.

ability on various grounds pertaining to the authenticity of the piece, to the source of the information or the chain of transmission, and to the procedure used to collect the evidence.

In *Tolimir*, for example, the accused challenged the reliability of satellite images, on the grounds that no evidence was presented concerning their origin, the method of their creation, the manner of their editing, how to interpret them or whether they were delivered to the Prosecution in their original form or in a modified version.[16] In *Ongwen*, the Defence contended that the majority of the intercepted material was irrelevant and that there were significant discontinuities in the tapes.[17] In the same case, it challenged the use of video footage as evidence, arguing that it was collected in violation of human rights and, therefore, as we will better explain here below, in contravention of the ICC Statute.[18] Human rights arguments were also raised in *Ayyash et a.* concerning the admissibility into evidence of call sequence tables, which were gathered, according to the Defence, in violation of the right to privacy.

3. QUESTIONS OF ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE BEFORE INTERNATIONAL CRIMINAL TRIBUNALS

The Statutes of the international criminal tribunals do not contain any specific provision on digital evidence, which is also not defined by their rules of evidence. Concerning its admissibility, the Rules of Procedure and Evidence (RPE) of international tribunals do not include specific provisions on this particular type of evidence, the admissibility and reliability of which are therefore governed by general norms. These grant judges a broad margin of discretion in the matter.

Rule 89 (C) of the ICTY and of the International Criminal Tribunal for Rwanda (ICTR) give the Chamber the power to admit any relevant evidence which it deems to have probative value.[19] Article 89(D) of the ICTY RPE further provides that a Chamber may exclude evidence if its probative value is substantially out-

---

16 *Tolimir*, *op. cit.*, note 3, paras. 67-68. The Prosecutor was actually not allowed to share any information relating to the "technical or analytical sources, methods, or capabilities of the systems, organizations, or personnel used to collect, analyse, or produce these imagery-derived products".

17 *Prosecutor v Ongwen*, Case No. ICC-02/04-01/15, Public Redacted Version of 'Corrected Version of "Defence Closing Brief", 13 March 2020, paras. 232-233.

18 *Ongwen*, *op. cit.*, note 13, para. 54 ff.

19 International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994), IT/32Rev.50 (hereinafter 'ICTY RPE'); International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995), Rule 89(D).

weighed by the need to ensure a fair trial. The same principle has been applied by the ICTR, even if it is not expressly stated in its rules.[20]

Like the general ICTY and ICTR rules, Article 69(4) of the Rome Statute of the ICC provides that "the Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness […]". Article 69 (7) of Rome Statute specifies that "[e] vidence obtained by means of a violation of this Statute or internationally recognized human rights shall not be admissible if: (a) The violation casts substantial doubt on the reliability of the evidence; or (b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings". The same provisions are included in the STL Statute and in the RPE.[21] Although some slight differences exist among the evidentiary rules that each tribunal applies, some common principles may be inferred from the above provisions.

First, it is for the judges to rule on the admissibility and relevance of all evidence. In so doing, they may freely assess all types of evidence submitted, enjoying a significant degree of discretion. However, – and this is the second principle that may be drawn from the rules above - any item to be admitted as evidence must satisfy some requirements: i) relevance to the case, which shall be assessed, according to Articles 69(9)(a) and 69(4) of the ICC Statute, considering how much the "evidence tendered makes the existence of a fact at issue more or less probable"; ii) probative value, which points to its utility in proving an important part of the case and to its relevance in determining a fact or issue;[22] iii) both these conditions shall be balanced against any prejudicial effect that could be caused to the proceeding by the admission of the evidence. As to this last point, judges must be satisfied that, *inter alia*, evidence has not been obtained through means that amount to a violation of internationally recognized human rights, as this may jeopardize both its reliability and the integrity of the proceedings.

---

20 See on that the *Report on Digitally Derived Evidence In International Criminal Law*, Part of the digitally derived evidence Project, Leiden University, 2019, p. 22 ff., [https://leiden-guidelines.com/assets/DDE%20in%20ICL.pdf], Accessed 12 January 2023.

21 Art. 21 para. 2 states: "A Chamber may admit any relevant evidence that it deems to have probative value and exclude such evidence if its probative value is substantially outweighed by the need to ensure a fair trial". This provision is furtherly specified by Rule 162 RPE, that reads as it follows: "(A) No evidence shall be admissible if obtained by methods which cast substantial doubt on its reliability or if its admission is antithetical to, and would seriously damage, the integrity of the proceedings. (B) In particular, evidence shall be excluded if it has been obtained in violation of international standards on human rights, including the prohibition of torture".

22 Quelling, C., *The Future of Digital Evidence Authentication at the International Criminal Court*, Journal of Public & International Affairs, May 2022.

As mentioned above, digital evidence has been challenged in this last regard before the STL in *Ayyash et a.* and before the ICC in *Ongwen*.[23] In the former case, the Defence contended that the transfer of call data records from Lebanon to the United Nations International Independent Investigation Commission (UNIIIC), a commission established to investigate the murder of Rafiq Hariri, and to the Prosecution, was unlawful and arbitrary and that there had been violations of international human rights standards with regard to the right to private life. In *Ongwen*, the use of digital evidence was challenged on the grounds that it violated the right to a fair trial. It is worth noting that, in that case, the interceptions submitted by the Prosecutor were not made for purposes relating to a criminal investigation, but rather for security and military reasons. The materials transferred to the Prosecutor were, therefore, selected on the basis of the specific aim pursued by the Government, which was far from that of ensuring an objective investigation into the commission of international crimes; their admissibility as evidence raised human rights concerns in this regard with reference to due process standards.

3.1. Human rights standards and digital evidence

The law of evidence of international criminal tribunals generally refers to human rights standards without specifying further. This raises some questions about both which rights fall into the notion and their legal source.

The right to privacy is, as the cited cases clearly show, one of paramount concern when it comes to digital evidence, due to the fact that information is often collected using means that are likely to interfere in the private life of the person concerned. International criminal tribunals, starting with ICTY, have clearly stated that this right falls into the notion of "human rights standard" for the purposes of deciding on admissibility.[24] Concerning the legal source of the right, reference is generally made to Article 17 of the International Covenant on Civil and Political Rights, to Article 8 of the European Convention on Human Rights, and to Article 11 of the Inter-American Convention on Human Rights. According to the jurisprudence of both criminal and human rights tribunals, intercepts of private conversion and access to call data records may breach the right to privacy unless

[23] *Ongwen*, *op. cit.*, note 13, para. 57 ff.

[24] See for example *Ayyash* et al., *op. cit.*, note 12, para. 81; *Prosecutor v Radoslav Brdanin*, Case No. IT-99-36-T, Decision on the defence "objection to intercept evidence", 3 October 2003, spec. para. 31.; *Prosecutor v Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Decision on the confirmation of charges, 29 January 2007, para. 73, which reads as it follows: "…the right to privacy and to protection against unlawful interference and infringement of privacy is a fundamental internationally recognised right. However, it cannot be viewed as an absolute right in so far as these same instruments provide indications of what may be considered as a "lawful" interference with the fundamental right to privacy".

they respect certain guarantees.[25] The interception must be provided by the law, necessary under the circumstances, and proportional to the pursuit of a legitimate aim.[26] The European Court of Human Rights (ECtHR) has furtherly explained that the assessment shall be particularly rigorous where digital technologies are at issue. In *Amann v Switzerland*, it argued that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".[27] In *Centrum för Rättvisa v Sweden*, the ECtHR added, with regard to bulk interception, that "while Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present".[28]

Decisions on the admissibility of digital evidence that may raise human rights concerns should, therefore, be based on an overall assessment of whether the legal and procedural safeguards against abuse are sufficient and adequate.[29] In *Ayyash et*

---

25 *Malone v United Kingdom*, Application No. 8691/79, Judgment, 2 August 1984, para. 62; *Brđanin*, *op. cit.*, note 24, para. 30.

26 UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on State Party to the Covenant, CCPR/C/21/Rev.1/Add. 13, 24 May 2004, para. 6; ECtHR, *Amann v Switzerland* Application No. 27798/95, Judgment, 16 February 2000, para. 69, which expressely regards the consistency of interception of phone conversations with Article ECHR 8.

27 *Amann v Switzerland*, para. 56.

28 The Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: "(1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed". *Centrum För Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021, para. 178 ff.; in the same vein cf. [GC], *Big Brother Watch and Others v The United Kingdom*, Applications Nos. 58170/13, 62322/14, 24960/15, Judgment, 25 May 2021.

29 It is worth noting that recommendations on the necessity for States to adopt measures to ensure that the use of digital technologies does not affect human rights, and namely the right to private life was also issued by the UN General Assembly. On 18 December 2013 it adopted Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), in which, inter alia, it called upon States: "(a) To respect and protect the right to privacy, including in the context of digital communication; (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (c) To review their procedures, practices and legislation regarding the

al the STL admitted into evidence call records that were submitted by the Prosecutor on the grounds that they met the conditions required by international law to comply with human rights standards.[30]

The question then arises as to whether, in the opposite case, where the court concludes that digital evidence was obtained without respecting sufficient safeguards, this automatically renders evidence inadmissible or if there is room for balancing the seriousness of the human rights violation against the relevance of the proof in substantiating charges against persons convicted of international crimes. Both the ICC and the ICTY have taken the view that "the judges have the discretion to seek an appropriate balance between the Statute's fundamental values in each concrete case".[31]

In *Lubanga Dyilo*, the ICC Pre-Trial Chamber argued that, in the fight against impunity, it must ensure an appropriate balance between the rights of the accused and the need to respond to victims' and the international community's expectations. In the light of that, the judges decided that, although "the Items Seized were obtained without regard to the principle of proportionality and in violation of internationally recognised human rights", they should nevertheless be admitted into evidence as a result of the balance made between the seriousness of the violation and the fairness of the trial as a whole.[32] In making this decision, the ICC endorsed the approach taken some years before by the ECtHR. In *Shenk v Swtzerland*, the applicant complained about the use of a recording of his telephone conversations in the context of a criminal proceeding, arguing that the evidence had been obtained unlawfully and in violation of the right to private life. On the premise that questions regarding the rules on evidence admissibility fall outside the scope of its jurisdiction since it is for the State to legislate on

---

surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law".

30 *Ayyash et al*, *op. cit.*, note 12, para. 108.

31 *Brđanin*, *op. cit.*, note 24, where the point was made that "admitting illegally obtained intercepts into evidence does not, in and of itself, necessarily amount to seriously damaging the integrity of the proceedings". (*ibid.*, para. 61); *Prosecutor v Delalić et al.*, Case No. IT-96-21, Decision on the Motion of the Prosecution for the Admissibility of Evidence, 19 January 1998; *Prosecutor v Kordić and Cerkez*, Case No. IT-95-14/2-T, p. 13694, where it is stated that: "[…] evidence obtained by eavesdropping on an enemy's telephone calls during the course of a war is …not antithetical to and certainly would not seriously damage the integrity of the proceedings".
Lubanga Dyilo, op. cit., note 24, para. 74. See in this regard also Zappala, S., *Human Rights in International Criminal Proceedings*, Oxford University Press, Oxford, 2003. According to the author: "The approach adopted so far has been to admit any evidence that may have probative value, unless the admission of such evidence is outweighed by the need to ensure a fair trial" (*ibid.*, p. 149).

32 Lubnga Dyilo, *op. cit.*, note 24, para. 89 ff.

the matter in its discretion, the ECtHR stated that the admission into evidence of unlawfully collected information should not, *per se*, amount to a violation of the right to a fair trial. In order to ascertain whether such violation occurred, it went on, the judges must be satisfied, first, that the defendant did not have the opportunity to challenge the authenticity of the proof and to oppose its use, and, second, "that the recording of the telephone conversation was not the only evidence on which the conviction was based".[33]

In accordance with suggestions coming from human rights bodies, the International criminal tribunals generally favor corroboration of digital evidence through external indicators. External indicators include testimony[34] or information on the identity of the source, sometimes provided by experts, like in the *Ongwen* case, whereas internal indicators consisted of timestamps and metadata.[35] Concerning internal indicators, the ICC adopted an "e-Court Protocol", which provided specific standards of admissibility and reliability of digital evidence. To "ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings", the Protocol requires metadata to be attached, including the chain of custody in chronological order, the identity of the source, the original author and recipient of the information, and the author and recipient's respective organizations. However, as some scholars have correctly pointed out, "while the Protocol offers some guidance to facilitate the use of digital evidence, it is limited to harmonizing the format of digital evidence, and how it is stored in the Court's systems, and does not address issues of probative value of digital evidence",[36] nor the question of its compliance with human rights standards. It is worth noting that the lack of specific rules and guidelines for gauging the admissibility and weight of digital evidence may also impact the possibility for the defendant to contest its use in criminal proceeding and, therefore, bear on their right to a fair trial. This concern is heightened by the fact that defendants in general have limited resources compared with

---

33 *Schenk v Switzerland*, Application No. 10862/84, Judgment, 12 July 1988, para. 48. For a comment on the jurisprudence of the ECtHR in this regard see Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings,* Springer, Cham, 2020, pp.73-98; Thake, A. M., *The (In) Admissibility of Unlawfully Obtained Evidence at the International Criminal Court*, Hague Yearbook of International Law: Annuaire De La Haye De Droit International, Vol. 28, 2015, pp. 161-187.

34 See for example *Tolimir* in this regard.

35 On these aspects see *The working paper on "An Overview of the Use of Digital Evidence in International Criminal Courts"*, Salzburg workshop on cyberinvestigations, 2013, [https://humanrights.berkeley.edu/sites/default/files/publications/an-overview-of-the-use-of-digital-evidence-in-international-criminal-courts-salzburg-working-paper.pdf], Accessed 12 January 2023.

36 *Ibid.,* p. 4 ff.

those of the Office of the Prosecutor and may lack the technical ability required to properly challenge digital evidence on the basis of how it was collected.[37]

4. CONCLUDING REMARKS

The analysis conducted here illustrates the advantages and opportunities offered by digital technologies in the prosecution of international crimes, especially in the context of proceedings before international courts and tribunals, which, due to their temporal and geographical distance from crime scenes, may be at a disadvantage for fact-finding as compared with domestic courts.

Despite its relevance, however, digital evidence raises significant issues relating to reliability and admissibility. To overcome criticism about admitting evidence collected through information technologies, International criminal tribunals generally tend to require digital evidence to be accompanied by metadata and to be, in the most controversial cases, corroborated by witness testimony. The same approach can be found *a fortiori* in cases where challenges to the admissibility of evidence are grounded on human rights considerations. As the jurisprudence of the ECtHR also shows, the use of technological devices for gathering information may, in fact, raise concerns relating to the right to private life. It is worth noting, however, that not all interferences in the life of individuals necessarily amount to a breach of the right, provided that they are justified by security reasons or that they are necessary to investigate the commission of a crime.

Even in cases where a violation has occurred, this alone is not sufficient to render the evidence inadmissible. In these cases, judges must rather assess the impact on the reliability of the evidence and on the integrity of the proceedings as a whole. This implies that the use of technology for investigation purposes must be evaluated against due process standards. To that end, some scholars suggest that the international criminal tribunals develop specific guidelines and rules to address the digital evidence and to overcome the limits of old procedural guarantees, developed at a time when the use of modern technologies was still highly unusual.[38] Although the ICC has taken some steps in this regard, through the adoption of the "E-court Protocol" and through the appointment of a Scientific Advisory Board to assist the Office of Prosecutor in verifying the authenticity and reliability of the evidence, further efforts must be made to revise procedural rules, in order

---

[37] On this issue and more generally for a recent critical analysis on the relevance of human rights standards of fair trial in the jurisprudence of the ICC, see De Arcos Tejerizo, M., *Digital evidence and fair trial rights at the International Criminal Court,* Leiden Journal of International Law, Vol. 36, No.3, 2023, pp. 749-769.

[38] See Freeman, L., *op. cit.*, note 6, p. 64.

to ensure that the rights of all parties are fully guaranteed.[39] Only in this way will digital evidence, with all its great potential for prosecuting the worst violations of human dignity that amount to international crimes, provide support for the pursuit of justice rather than risk undermining the perception of its fairness and credibility.

REFERENCES

BOOKS AND ARTICLES

1. De Arcos Tejerizo, M., *Digital evidence and fair trial rights at the International Criminal Court,* Leiden Journal of International Law, Vol. 36, No.3, 2023, pp. 749-769
2. Freeman, L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal, Vol. 41, No. 2, 2018, pp. 283-336
3. Freeman, L., *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in: Dubberley, S.; Koenig, A.; Murray, D. (eds.), Digital Witness - Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67
4. Freeman, L.; Vazquez Llorente, R., *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188
5. Fremuth, M., *Prosecutor v. Ayyash et al (Special Trib. Leb.)*, International Legal Materials, Vol. 60, No. 3, 2021, pp. 357-447
6. Harmon, M.B., *Prosecuting Massive Crimes with Primitive Tools: Three Difficulties Encountered by Prosecutors in International Criminal Proceedings*, Journal of International Criminal Justice, Vol. 2, No. 2, 2004, pp. 403–426
7. Hellwig, K., *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings,* International Criminal Law Review, Vol. 22, No. 5-6, pp. 965-988
8. Land, M.; Aronson, J. (eds.), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018
9. Marchesi, D., *Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC*, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940
10. Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings,* Springer, Cham, 2020
11. Quelling, C., *The Future of Digital Evidence Authentication at the International Criminal Court*, Journal of Public & International Affairs, May 2022.
12. Roscini, M., *Digital Evidence as a Means of Proof before the International Court of Justice*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 541-554

[39] In this vein see Hellwig, K., *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings,* International Criminal Law Review, Vol. 22, No. 5-6, pp. 965-988.

13. Sandalinas, J., *Satellite Imagery and its use as Evidence in the Proceedings of the International Criminal Court*, Zeitschrift Für Luft-Und Weltraumrecht: Vierteljahresschrift Des Instituts Für Luft- Und Weltraumrecht Der Universität Köln, Vol. 64, No. 4, 2015, pp. 666-675
14. Thake, A. M., *The (In)Admissibility of Unlawfully Obtained Evidence at the International Criminal Court*, Hague Yearbook of International Law: Annuaire De La Haye De Droit International, Vol. 28, 2015, pp. 161-187
15. Zappala, S., *Human Rights in International Criminal Proceedings*, Oxford University Press, Oxford, 2003

ECHR

1. *Schenk v Switzerland*, Application No. 10862/84, Judgment, 12 July 1988
2. *Amann v Switzerland*, Application No. 27798/95, Judgment, 16 February 2000
3. *Centrum För Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021
4. *Big Brother Watch and Others v The United Kingdom*, Applications Nos. 58170/13, 62322/14, 24960/15, Judgment, 25 May 2021
5. *Malone v United Kingdom*, Application No. 8691/79, Judgment, 2 August 1984

INTERNATIONAL CRIMINAL COURT

1. *Prosecutor v Al Mahdi*, Case No. ICC-01/12-01/15-171, Decision on the confirmation of charges against Ahmad Al Faqi Al Mahdi, 24 March 2015
2. *Prosecutor v Dominic Ongwen*, Case No. ICC-02/04-01/15, Judgment, 4 February 2021
3. *Prosecutor v Ongwen, Case* No. ICC-02/04-01/15, Public Redacted Version of 'Corrected Version of "Defence Closing Brief", 13 March 2020
4. *Prosecutor v Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Decision on the confirmation of charges, 29 January 2007

INTERNATIONAL CRIMINAL TRIBUNAL FOR RWANDA

1. International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995)
2. *Prosecutor v Bagosora*, Case No. ICTR-98-41-T, Trial Judgment and Appeals Judgment, 8 December 2008 and 14 December 2011

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA

1. *Prosecutor v Blagojević and Jokić*, Case No. IT-02-60-T, Decision on the admission into evidence of intercept-related materials, 18 December 2003
2. *Prosecutor v Delalić et al.*, Case No. IT-96-21, Decision on the Motion of the Prosecution for the Admissibility of Evidence, 19 January 1998
3. *Prosecutor v Kordić and Cerkez*, Case No. IT-95-14/2-T

4. *Prosecutor v Popović et al*, Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, 7 December 2007
5. *Prosecutor v Radoslav Brdanin*, Case No. IT-99-36-T, Decision on the defence "objection to intercept evidence", 3 October 2003
6. *Prosecutor v Radislav Krstic*, Case No. IT-98-33, Judgement, 2 August 2001
7. *Prosecutor v Tolimir*, Case No. IT-05-88/2-T, Judgment, 12 December 2012
8. International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994)

SPECIAL TRIBUNAL FOR LEBANON

1. *Prosecutor v Ayyash et al*, Case No. STL-11-01, Decision on Motions for the Admission of the Call sequence tables related to the five colour-coded mobile telephone groups and networks, 31 October 2016

UNITED NATIONS

1. International Commission of Inquiry on Darfur, *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General*, 2005, [https://www.legal-tools.org/doc/1480de/pdf/], Accessed 12 January 2023
2. UN General Assembly, Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), 18 December 2013
3. UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on State Party to the Covenant (CCPR/C/21/Rev.1/Add 13), 24 May 2004

REPORTS

1. European Commission, *European Data Informatics Exchange Framework for Courts and Evidence*, European Evidence Project, available online at [www.cordis.europa.eu/project/id/608185/reporting/de], Accessed 12 January 2022
2. Leiden University, *Report on Digitally Derived Evidence In International Criminal Law*, Part of the digitally derived evidence Project, 2019, [https://leiden-guidelines.com/assets/DDE%20in%20ICL.pdf], Accessed 12 January 2023
3. *The working paper on "An Overview of the Use of Digital Evidence in International Criminal Courts"*, Salzburg workshop on cyberinvestigations, 2013, [https://humanrights.berkeley.edu/sites/default/files/publications/an-overview-of-the-use-of-digital-evidence-in-international-criminal-courts-salzburg-working-paper.pdf], Accessed 12 January 2023

UDK 343.549-053.2:341.9]:004
347.63:341.9]:004
Original scientific paper

INTERNATIONAL FAMILY LAW IN THE AGE OF DIGITALISATION: THE CASE OF CROSS-BORDER SURROGACY AND INTERNATIONAL PARENTAL CHILD ABDUCTION*

Katarina Trimmings, PhD, Professor
University of Aberdeen, School of Law
High Street, Aberdeen, AB24 3UB, United Kingdom
k.trimmings@abdn.ac.uk

ABSTRACT

This article illustrates in an anecdotal way the impact of digitalisation on international family law. Specifically, it explores the part that digital technologies have played in the expansion of cross-border assisted reproduction, with a particular focus on cross-border surrogacy arrangements. It then examines the interface between international parental child abduction and facial recognition technologies. The EU approach to the use of AI-powered facial recognition technologies is explained, before considering the potential utility of facial recognition technologies in the specific context of international parental child abduction.

Keywords*: International Family Law, digitalisation, cross-border surrogacy, facial recognition, digital technologies, international parental child abduction*

1. INTRODUCTION

In one way or another, developments in the area of digital technologies over the past few decades have affected every area of law, including international family law. This article maps the impact that digital technologies have had on international family law in two distinct respects. First, it explains the role that the internet and other digital channels of communication such as smartphones (text and video messaging), social media, and applications such as WhatsApp have played in the

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

growth of cross-border assisted reproduction. The legal consequences of this trend are then demonstrated using the example of cross-border surrogacy arrangements. Second, the article explores the interface between international parental child abduction and facial recognition technologies. The EU approach to the use of facial recognition technologies in the context of legal proceedings is discussed before considering the potential utility of these AI technologies in the specific context of international parental child abduction.

Cross-border surrogacy and international parental child abduction have been at the centre of the author's research over the past decade. In the course of her involvement in the DIGinLaw project from which this special issue stems, the author developed strong interest in digitalisation and the impact that digitalisation has had on different areas of law. This intellectual curiosity naturally led to a desire to explore the role of digitalisation within in her key areas of expertise – cross-border surrogacy and international parental child abduction. It should be noted that the underlying objective of the article is to exemplify the impact of digitalisation on international family law, without aiming to cover the topic in an exhaustive way or seeking to offer detailed solutions to the issues identified throughout the analysis.

2. DIGITAL TECHNOLOGIES AND CROSS-BORDER ASSISTED REPRODUCTION

It is more and more common for the delivery of healthcare to be facilitated by digital channels such as the Internet, smartphones (text and video messaging), social media, multi-platform instant messaging and voice-over-IP service apps (such as WhatsApp and Telegram) and telemedicine. This trend has been enabled by dispersion of mobile technology and rapid advances in artificial intelligence. Digital communication channels provide wide coverage, enable communication, including (often untrustworthy) advertising and information sharing to be directed at specific groups or individuals. The area of reproduction is no exception to this trend. Quite the contrary - the employment of assisted reproduction technologies combined with the use of the Internet[1] and other digital communication channels has led to the proliferation of modern family building methods. Traditionally, conception occurred through sexual intercourse between a male and female, with the male supplying the sperm and the female providing the ova. Assisted reproductive technologies ('ART') is the overarching term for various medical technolo-

[1] For an overview of concerns surrounding the use of the Internet in the context of cross-border assisted reproduction see Hird Chung, L., *Free Trade in Human Reproductive Cells: A Solution to Procreative Tourism and the Unregulated Internet*, Minnesota Journal of International Law, Vol. 15, 2006, pp. 263-296, 283-284.

gies that are employed to achieve conception through means other than sexual reproduction.[2] There are various ART techniques. The oldest and most common is Artificial Insemination ('AI'), followed by In Vitro Fertilization ('IVF').[3] These procedures aim at a successful fertilization of a human ova, with the view of creating an embryo. That embryo may then be stored for future use or implanted into a woman's uterus for gestation.[4] Gestation may be facilitated by a surrogate mother.[5] Over the past few decades, there has been a significant growth in ART practices using gamete or embryo donation and/or employing the services of surrogate mothers. The Internet and other technological developments have walked hand in hand with the growth of ART as potential 'suppliers' and 'consumers' are now able to connect in ways that were inconceivable in the past when the only avenue to advertise for gamete donors was through local newspapers.[6] In the context of surrogacy in particular, the Internet has played a significant role in this process as it has facilitated the making of surrogacy arrangements between adults – either directly[7] or via intermediaries.[8] In this regard, justified concerns have been expressed about the lack of legal regulation of such activities on the Internet and the potential for legal disputes further down the line.[9]

---

2 For a detailed overview of ART methods and recent trends in the field see e.g., Sheriff, D.S. (ed.), *Infertility, Assisted Reproductive Technologies and Hormone Essays*, IntechOpen, London, 2019.

3 See e.g., Dale, B.; Elder, K., *In Vitro Fertilisation*, Cambridge University Press, Cambridge, 1997; and Meniru, G.; Brinsden P.; Craft I., *A Handbook of Intrauterine Insemination*, Cambridge University Press, Cambridge, 1997.

4 For an overview of global embryo disposal practices and trends see Simopoulou, M. *et.al.*, *Discarding IVF Embryos: Reporting on Global Practices*, Journal of Assisted Reproduction and Genetics, Vol. 36, 2019, pp. 2447–2457.

5 Generally, see Trimmings, K.; Shakargy, S.; Achmad C., *Research Handbook on Surrogacy and the Law,* Edward Elgar Publishing, Cheltenham, 2024 (forthcoming).

6 See e.g., Storrow, R., *Quests for Conception: Fertility Tourists, Globalization and Feminist Legal Theory*, Hastings Law Journal, Vol. 57, 2006, pp. 295-330, who explores the dynamics of reproductive tourism in the globalization era.

7 See e.g., *Re A* [2014] EWFC 55 [1]: 'The adults met via an internet website upon which Wendy had posted her details effectively offering herself as a surrogate. AC [the intended mother] saw those details and contacted Wendy and the matter swiftly proceeded from there. […] An arrangement was reached between Wendy, AC and JD [the intended father] in 2012 that Wendy would carry a child for them using her own egg and JD's sperm.' Relevant groups can be hosted also on social media platforms such as Facebook. See e.g., *Re Z (A Child)* [2016] EWFC 34 [2]: 'The applicants, who are a same sex couple, were introduced to X through a Facebook surrogacy site, which was run or administered by W and others, to provide a forum for the introduction of potential surrogates and commissioning parents.'

8 In the UK, for example, negotiating a surrogacy arrangement on a commercial basis is a criminal offence, nevertheless, a number of agencies have been set up to facilitate surrogacy arrangements by making introductions, and providing advice and counselling to the parties: e.g, COTS Surrogacy UK, [https://www.surrogacy.org.uk/]; and Brilliantbeginnings, [https://brilliantbeginnings.co.uk/].

9 See e.g., an informal surrogacy arrangement case of *Re T (a child) (surrogacy: residence order)* [2011] EWHC 33 (Fam) [38], which involved a dispute between the intended parents and the surrogate

While many couples and individuals might need reproductive assistance in the form of gametes, embryos or surrogacy services, such assistance may be restricted or banned by the laws of their home countries. This leads to such persons bypassing the laws of their home countries by seeking reproductive assistance abroad. Other reasons for travelling abroad for reproductive treatment include possible unavailability or unaffordability of such treatment in one's home jurisdiction, lengthy waiting lists or simply convenience.[10] The practice of travelling for fertility treatment abroad is referred to as 'reproductive tourism' (also known as 'fertility tourism', 'procreative tourism' or 'cross-border reproductive care').[11] Technological advances have facilitated the development of reproductive tourism and cross-border family building using assisted reproduction.[12] As a result, the cross-border surrogacy market as well as the market in human gametes and, to a lesser extent, embryos, have grown exponentially over the past few decades.[13] Among the multitude of such cases worldwide, this reality is well illustrated by a UK cross-border surrogacy case of *Z and another v C and another.*[14] This case concerned a set of twins who had been conceived as a result of a surrogacy agreement between the intended parents (a same-sex male couple) and a clinic in India, arranged through a surrogacy agency based in Israel. The surrogate mother was Indian, one of the intended fathers was the genetic father and the egg donor originated from South Africa.[15] Being con-

---

mother over the custody of the surrogate-born child. In this case, the judge rightly expressed concerns 'about the dangerous and murky waters into which they [the parties] have strayed via the internet.' The parties had come across each other on an internet surrogacy site and connected in an internet chatroom. Prior to the intended parents entering into the arrangement with the surrogate mother, they had met another woman on an internet surrogacy site. That woman was already pregnant, and the intended parents most likely intended to buy the baby that she was carrying. This plan was aborted by the social services that later discovered that the woman was 'a prostitute, with seven children in care in Scotland', who was 'known on the internet as a surrogate parent […].' Ibid [40].

10 For a taxonomy of types of medical tourism see Cohen, G., *Patients with Passports*, Oxford University Press, Oxford, 2015, pp. 1-16.

11 See e.g., Ikemoto, L.C., *Reproductive Tourism Equality Concerns in the Global Market for Fertility Services*, in: Obasogie, O.K.; Darnovsky, M. (eds.), *Beyond Bioethics: Toward a New Biopolitics*, 2018, pp. 339 – 349; Pennings, G., *Legal Harmonization and Reproductive Tourism in Europe*, Reproductive Health Matters, Vol. 13, No. 25, 2005, pp. 120–128; and Deech, R., *Reproductive Tourism in Europe: Infertility and Human Rights*, Global Governance, Vol. 9, No. 4, 2003, pp. 425–432. On the moral aspects of reproductive tourism see Pennings, G., *Reproductive Tourism as Moral Pluralism in Motion*, Journal of Medical Ethics, Vol. 28, No. 6, 2002, pp. 337–341.

12 Sometimes, crafty intermediaries attract exhausted infertile couples or individuals by offers of ART treatments combined with vacations ('fertility holidays'). See Speier, A., *Fertility Holidays: IVF Tourism and the Reproduction of Whiteness*, New York University Press, New York, 2016.

13 For more details on these forms of reproductive tourism see e.g., Vida, P., *Surrogate Tourism and Reproductive Rights*, Hypatia, Vol. 28, No. 2, 2013, pp. 274–289.

14 *Z and another v C and another* [2011] EWHC 3181 (Fam).

15 *Ibid.* [2].

fronted by cases such as this, it is no exaggeration to say that we are living in the cyberprocreation era.[16]

More often than not, those engaging in reproductive tourism do not have the advantage of the reliable legal advice, counselling and support.[17] This is true in particular in relation to cross-border surrogacy arrangements. Unregulated form of surrogacy means that there are on the one side vulnerable surrogates, and on the other intended parents who are legally unprotected from unpredictable outcomes. Ethical concerns[18] aside, cross-border surrogacy arrangements, raise serious legal problems. Among these, the most salient is the question of recognition in the country of residence of the intending parent(s) of legal parenthood established in the country of birth. International and regional organisations have responded cautiously to the practice of cross-border surrogacy and emphasised the need to regulate the practice. In 2019, the UN Special Rapporteur on the sale of the child expressed concerns about the practice of cross-border commercial surrogacy in a Report presented to the Human Rights Council.[19]

At the same time, legislative endeavours to address private international law issues concerning children born through cross-border surrogacy have been ongoing since 2011 at the Hague Conference on Private International Law ('HCCH'),[20] whilst the jurisprudence of the European Court of Human Rights ('ECtHR' or 'the Court') on cross-border surrogacy dates back to 2014, when the pivotal case of *Mennesson v France*[21] reached the Court. It has been followed by a number of

---

16 See Swink D.; Reich, B., *Outsourcing Reproduction: Embryos and Surrogacy Services in the CyberProcreation Era*, Ethics and Business Law Faculty Publications, Vol. 14, 2011, pp. 1-62.

17 See comment by Baker J in *Re T (a child) (surrogacy: residence order)* [2011] EWHC 33 (Fam) [2].

18 Deonandan, R.; Green, S.; van Beinum, A., *Ethical Concerns for Maternal Surrogacy and Reproductive Tourism*, Journal of Medical Ethics, Vol. 38, 2012, pp. 742-745.

19 UN Special Rapporteur on the Sale of the Child, *Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material*, A/74/162, 2019, [https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/216/49/PDF/N1921649.pdf?OpenElement], Accessed 20 July 2023. In the Report, the Special Rapporteur noted the presence of abusive practices in both unregulated and regulated contexts and expressed concerns that the practice of engaging surrogate mothers in States with emerging economies to bear children for more wealthy intending parents from other States entails power imbalances and presents risks for both the children and surrogate mothers.

20 See Hague Conference on Private International Law, Parentage / Surrogacy Project, 2011-to date, [https://www.hcch.net/en/projects/legislative-projects/parentage-surrogacy], Accessed 20 July 2023.

21 *Mennesson v France*, Application No. 65192/11, ECHR 2014 (extracts). Decided jointly with the case of *Labassee v France*, Application No. 65941/11, 26 June 2014. The ECtHR faced the question of the inability of children born in a foreign jurisdiction through a gestational surrogacy arrangement and their intended parent(s), to obtain recognition in the country of residence of the intended parent(s) of the parent-child relationship legally established between them in the country of birth. The Court ruled that the child's right to respect for his or her private life, which encompasses the right to identi-

other cases involving surrogacy arrangements with a cross-border element.[22] It is beyond the scope of this paper to analyse the work of the HCCH or the ECtHR case-law; the aim is to merely illustrate the policy consequences of the complexities of cross-border reproduction in the era of modern technologies.

3. INTERNATIONAL PARENTAL CHILD ABDUCTION AND FACIAL RECOGNITION TECHNOLOGIES

This section explores the interface between facial recognition technology ('FRT') powered by artificial intelligence ('AI')[23] and international parental child abduction. The section starts with a brief overview of the EU policy on the use of the FRT, and the fundamental rights considerations that surround the use of FRT, including by the public sector, law enforcement and border management. It then sets out the instruments that govern parental child abduction in the EU, before considering whether, in the light of the fundamental rights and other considerations, it would be appropriate to use FRT to locate abducted children and abducting parents in the EU in proceedings for the return of abducted children under the 1980 Hague Convention on the Civil Aspects of International Child Abduction.

3.1. Facial recognition in the EU

Facial recognition technology (FRT)[24] makes it possible 'to detect, identify and verify a person or an object from a digital image or video footage based on specific

---

ty, required that domestic law provide a possibility of recognition of the legal relationship between a child born through a surrogacy arrangement abroad and the intended father, where he is the biological father. The Court emphasised that 'respect for private life require[d] that everyone should be able to establish details of their identity as individual human beings, which include[d] the legal parent-child relationship' and that 'an essential aspect of the identity of individuals [was] at stake where the legal parent child relationship [was] concerned'. *Mennesson v France* [96].

22 An overview of the ECtHR case law can be found here: European Court of Human Rights, Press Unit, *Factsheet – Gestational Surrogacy*, 2022, [https://www.echr.coe.int/Documents/FS_Surrogacy_eng.pdf], Accessed 19 July 2023. For a more detailed analysis see e.g., Trimmings, K., *Surrogacy Arrangements and the Best Interests of the Child: The Case Law of the European Court of Human Rights* in: Bergamini, E.; Ragni, C., *Fundamental Rights and Best Interests of the Child in Transnational Families*, Intersentia, Cambridge, 2019, pp. 187-207; Cammu, N.; Vonk, M., *The Significance of Genetics in Surrogacy* in: Trimmings *et al., op. cit.,* note 5; and Tryfonidou, A., *Surrogacy in the ECtHR and European Institutions* in: Trimmings *et al., op. cit.,* note 5.

23 For a detailed analysis of various aspects of artificial intelligence see Barfield, W.; Pagallo, U., (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Cheltenham, 2018.

24 For a detailed overview of face recognition systems see Adjabi, I., *et al.*, *Past, Present, and Future of Face Recognition: A Review*, Electronics, Vol. 9, No. 8, 2020, p. 1188.

facial or other features.'[25] It enables the comparison of digital facial images with the view of establishing whether they are of the same person.[26] When footage obtained from video cameras (CCTV) deployed in public spaces is compared with images in databases, this is known as 'live facial recognition technology'.[27] In the EU, the discussion about facial recognition technology has grown considerably in recent years. As the technology becomes more advanced, concerns have been raised in terms of surveillance, privacy, consent, accuracy and bias.

3.1.1. EU Fundamental Rights Agency: key considerations

In its 2019 Focus Paper,[28] the EU Fundamental Rights Agency set out the key aspects that must be considered before deploying facial recognition technologies in real life applications.

First, a clear and sufficiently detailed legal framework must regulate the deployment and use of facial recognition technologies. In deciding when the processing of facial images is necessary and proportionate, the following two issues have to be considered: first, the purpose for which FRT is being utilised; and second, the protections in place to safeguard persons whose facial images are being processed from adverse effects. [29] Forms of facial recognition that involve a very high degree of intrusion into fundamental rights are unlawful.

Second, the processing of facial images for verification purposes must be distinguished from the processing of facial images for identification purposes.[30] The former means that two facial images are compared to determine if they are of the same person whereas the latter occurs when 'a facial image is run against a database or watchlist of facial images'.[31] This distinction is important as the processing of

---

25 European Commission, *Study on the Use of Innovative Technologies in the Justice Field*, 2020, p. 13, [https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1], Accessed 20 July 2023. For a detailed overview of FRT that links the technical and the socio-political discourse on the topic see Introna, L.; and Nissenbaum, H., *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030, [https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf], Accessed 10 May 2023.

26 O'Flaherty, M., *Facial Recognition Technology and Fundamental Rights*, European Data Protection Law Review, Vol. 6, 2020, pp. 170-173, 170.

27 *Ibid*.

28 European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, 2019, [https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law], Accessed 12 March 2023.

29 *Ibid.*, p. 33.

30 *Ibid*.

31 *Ibid*.

facial images for identification purposes carries a higher risk of interference with fundamental rights, and therefore, the necessity and proportionality assessment must be more rigorous.

Third, so-called 'live facial recognition technologies' are particularly challenging. This form of employment of FRT raises concerns over imbalance of power between the State and the citizen. These concerns must not be underestimated, especially as citizens are likely to be unaware that their facial image is being compared against a database/watchlist and considering the higher level of error when compared to the use of facial images taken in controlled environment (e.g., a police station).[32] Therefore, 'live facial recognition technologies' should not be routinely employed, and their use should be 'strictly limited to combatting terrorism and other forms of serious crime, or to detect missing people and victims of crime.'[33]

Fourth, FRT algorithms provide only probabilities that two images are of the same person; they do not give a conclusive result. In the law enforcement sphere, there is therefore a possibility that a person will be erroneously flagged. Such incidents must be curtailed, and persons identified by the technology must be 'treated in a dignified in manner'.[34]

Fifth, public authorities normally entrust the development and procurement and of FRTs to private companies. In this process, such companies such be contractually bound to build fundamental rights considerations into technical specifications of the technologies they develop and/or procure.[35] It is imperative to ensure that data protection and non-discrimination requirements in particular are placed at the centre of all technical specifications.[36]

Sixth, it is essential that a fundamental rights impact assessment is carried out invariably with the view of guaranteeing a fundamental rights compliant application of FRTs in all contexts.[37] This assessment must cover in a comprehensive way all the rights that are potentially affected, and private companies should provide

---

32 *Ibid.*, p. 34.

33 *Ibid*.

34 *Ibid*.

35 *Ibid*.

36 See also Castelluccia, C.; Le Métayer Inria, D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, Centre for Data Ethics and Innovation, 2020, [https://inria.hal.science/hal-02480647/document], Accessed 14 April 2023. The authors suggest that standards for the testing, validation and certification of FRT should be clearly defined and verifiable by independent third parties. They should provide 'guarantees regarding the compliance of these systems with essential requirements, for example in terms of accuracy, absence of bias and database security.'

37 European Union Agency for Fundamental Rights, *op. cit.,* note 28, p. 34. See also Castelluccia *et al., op. cit.,* note 36. For an example in a related area see e.g., privacy impact assessment tool proposed by

public authorities with all necessary information.[38] Trade secrets or confidentiality considerations should not obstruct the process.[39]

3.1.2. Proposed Artificial Intelligence Act ('AI Act')

The proposed AI Act from April 2021[40] classifies different AI applications depending on their risks and implement varying degrees of restrictions.[41] The Proposal considers AI under four different categories: unacceptable risk, high-risk, limited risk and minimal risk.[42] In cases of unacceptable risk, AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned.[43] This includes so-called social credit scores, such as a controversial system seen in China, and applications that can be seen as manipulating human behaviour.[44] Facial recognition falls within the next category - i.e., high-risk. High-risk cases include the use of AI in critical infrastructure, law enforcement, migration and border patrol, employment and recruitment, and education.[45] The proposal requires that these applications implement strict security controls, maintain logs of how the

---

the French Data Protection Agency (CNIL), *Privacy Impact Assessment (PIA)*, [https://www.cnil.fr/en/privacy-impact-assessment-pia], Accessed 20 July 2023.

38 Castelluccia *et al., op. cit.,* note 36.

39 *Ibid*. See also Council of Europe Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, 2019, [https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64], Accessed 20 July 2023.

40 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 ('AI Act Proposal'). In addition to the proposed AI Act, the EU legal framework pertinent to facial recognition includes the so-called Law Enforcement Directive (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA). This instrument applies to both domestic and cross-border processing of personal data by competent authorities to prevent, investigate, detect or prosecute criminal offences and execute criminal penalties, including safeguarding against and preventing threats to public security.

41 For a detailed analysis of the proposed Regulation see e.g., Veale, M.; and Zuiderveen Borgesius, F., *Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, Computer Law Review International, Vol. 22, No. 4, 2021, pp. 97-112.

42 For a detailed analysis see European Parliament, Regulating Facial Recognition in the EU, 2021, pp. 24-31, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf], Accessed 20 July 2023.

43 European Commission, *Regulatory Framework Proposal on Artificial Intelligence*, [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], Accessed 13 May 2023.

44 Cheung, A.; and Chen, Y., *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, Law & Social Inquiry, Vol. 47, No. 4, 2022, pp. 1137-1171.

45 AI Act Proposal, *op. cit.,* note 40, Annex III.

technology is used for auditing,[46] and provide data to users on how the AI operates. Furthermore, it requires some human oversight of the technology in use.[47] This category still allows for the use of (so called) 'remote biometric identification systems', such as live facial recognition, subject to strict requirements.[48] Live use of this technology in publicly accessible spaces for law enforcement purposes is prohibited in principle, but narrow exceptions are strictly defined and regulated.

The bill is currently being amended by members of the European Parliament and EU Member States. The negotiations have seen a fierce debate over the use of facial recognition technologies.[49] Some MEPs and civil society organisations are of the view that, given the inherent risks of violations of fundamental rights, the AI Act should ban the use of facial recognition in public places.[50] This view is shared by some EU Member States. For example, Germany has said that it supports a full ban on the use of facial recognition in public places.[51] Other countries such as France, want to make exceptions for using facial recognition to protect national security.[52]

It is essential that the European legislator gets this right, not only in order to ensure the protection of the safety and fundamental rights of EU citizens but also because the EU is aspiring to lead the development of new global norms to make sure AI can be trusted. It is hoped that by setting the standards, the EU can pave the way to ethical technology worldwide.

3.1.3. Fundamental rights considerations

Recent developments in the field of AI powered FRT are not only of a potential use to private enterprises but are of interest also to the public sector, law enforcement and border management not excluding.[53] Such application scenarios include for example situations where a FRT would identify individuals in a crowd, and being connected to video surveillance systems (CCTV) monitoring outdoor areas,

---

46 *Ibid.*, Art 12.

47 *Ibid.*, Art 14.

48 *Ibid.*, Art 5(1)(d).

49 For a detailed analysis see European Parliament, *op. cit.,* note 42, p. 34.

50 European Digital Rights (EDRi), *Will the European Parliament Stand Up for Our Rights by Prohibiting Biometric Mass Surveillance in the AI Act?*, 2022, [https://edri.org/our-work/will-the-european-parliament-stand-up-for-our-rights-by-prohibiting-biometric-mass-surveillance-in-the-ai-act/], Accessed 10 April 2023.

51 Politico, *Europe Edges Closer to a Ban on Facial Recognition*, 2022, [https://www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/#:~:text=And%20while%20the%20European%20Commission,locating%20armed%20and%20dangerous%20criminals], Accessed 19 June 2023.

52 *Ibid*.

53 O'Flaherty *et al., op. cit.*, note 26.

the FRT system would alert authorities to the presence of a missing person/child.[54] In another typical application scenario, authorities may take advantage of control points set up at certain places such as passport inspection points or security checkpoints at airports, where agents may intentionally or inadvertently compel the passengers to make eye contact, which is likely to result in a higher success of the true identity verification of the subject than in the previous application scenario.[55] When footage obtained from video cameras (CCTV) is compared with images in databases, this is known as 'live facial recognition technology'.[56]

Recent technological developments have resulted in increased accuracy of FRTs. This in turn has encouraged many public authorities across the world to start using, testing or planning the use of FRTs. For example, the police in the United Kingdom carried out several tests in real life situations such as sports events, even using real watch lists. Other law enforcement agencies tested the accuracy of the technology in larger tests with volunteers, such as the police in Berlin, Germany or in Nice, France.[57]

Using FRT affects a range of fundamental rights, and a number of questions arise from a fundamental rights perspective: is this technology appropriate for law enforcement and border management use? Which fundamental rights are most affected when this technology is deployed? What measures should public authorities take to guarantee that these rights are not violated?

The fundamental rights repercussions of using FRT differ substantially depending on the objective, context and extent of the employment of such technologies. Some of the fundamental rights concerns are caused by FRT's lack of accuracy.[58] For

---

54 Introna *et al., op. cit*., note 25, p. 20.

55 *Ibid.*

56 O'Flaherty *et al., op. cit*., note 26.

57 During the Nice carnival in February 2019: see Ville de Nice, *Rapport: Experimentation Reconnaissance Faciale*, 2019, [https://s3.documentcloud.org/documents/6350838/Bilan-Reconnaissance-Faciale.pdf], Accessed 15 April 2023.

58 In this context, it has been suggested that '[i]t will still be some time before FRT will be able to identify "a face in the crowd" (uncontrolled environments) with any reasonable level of accuracy and consistency. It might be that this is ultimately an unattainable goal, especially for larger populations. […] with large populations it will create many biometric doubles that then need to be sorted out using another biometric.' Introna *et al., op. cit*. note 25, p. 46. To this effect, some commentators have argued for multi-modal biometric systems, e.g., merging of face recognition with gait recognition (or even voice recognition) to carry out identification at a distance. Ibid. See also Goldenfein, J., *Facial Recognition is Only the Beginning*, 2020, [https://www.publicbooks.org/facial-recognition-is-only-the-beginning/], Accessed 12 April 2023. Crumpler W., *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, 2020. [https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it], Accessed 20 July 2023. Schneier, B., *We Are Banning*

example, FRT has higher error rates when used on women and people of colour, which raises concerns over gender and racial bias similar to controversial practices such as racial profiling.[59] This can eventually lead to discrimination,[60] suggesting that 'such systems do not belong in societies with aspirations of egalitarianism.'[61] But, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors. For instance, the way facial images are obtained and used - potentially without consent or opportunities to opt out - can have a negative impact on people's dignity. Meaningful consent 'recognises subjects as decision makers by providing them information and the capacity to accept or reject conditions of the system (for example, allowing people to opt out of a particular service or place if it requires enrolment in a system and identification).'[62] This includes situations when an organisation or a state authority that has endorsed the use of FRT must enrol relevant persons, e.g., employees, customers, members into the system gallery. Is it ever appropriate to compel participation in such image databases?[63] Similarly, the use of facial recognition technology can also have a negative impact on the freedom of assembly and the freedom of expression, if people fear that facial recognition technology is being used to identify them ('chilling effect'). Inability to act as one wishes may not necessarily be of a concern if such conduct would be harmful to others; indeed, the values of freedom and autonomy would surely be trumped by a security threat.[64] Moreover, there are possible long-term implications. Curtailing privacy by processing large amounts of personal data, including in particular individual faces, may ultimately affect the functioning of democracy, since privacy is a core value inherent to a liberal democratic and pluralist society, and a cornerstone for the enjoyment of fundamental rights. Finally, in a more general sense, some academic commentators have suggested that the subjects of facial recognition both 'lack recognition for their individual uniqueness' as well as 'struggle to obtain adequate recognition on a universal level', arguing that these types of 'misrecognition' may impair a person's identity formation.[65]

The risk of errors in matching faces is the most frequently raised fundamental rights concern. However, fundamental rights concerns stem commonly also from

---

Facial Recognition. We're Missing the Point, New York Times, 20 January 2020, [https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html], Accessed 10 April 2023.

59 Introna *et al., op. cit.*, note 25, p. 45.

60 O'Flaherty *et al., op. cit.*, note 26, p. 171.

61 *Ibid*.

62 Introna *et al., op. cit.*, note 25, p. 46.

63 *Ibid.*

64 *Ibid*.

65 Waelen, A., *The Struggle for Recognition in the Age of Facial Recognition Technology*, AI Ethics, Vol. 3, 2023, pp. 215–222, following Charles Taylor's *The Politics of Recognition* (1992) and Axel Honneth's *The Struggle for Recognition* (1996).

the weak position of the individuals whose facial images are captured and processed. Fundamental rights affected include, among others, human dignity, the right to respect for private life, the protection of personal data,[66] non-discrimination, the rights of the child and the elderly, the rights of people with disabilities, the freedom of assembly and association, the freedom of expression, the right to good administration, and the right to an effective remedy and to a fair trial. All these rights are enshrined in international and regional human rights law, including the EU Charter of Fundamental Rights.

3.2. International parental child abduction

The key international instrument providing for a worldwide regulation of international parental child abduction is the 1980 Hague Convention on the Civil Aspects of International Child Abduction[67] ('the 1980 (Hague) Convention'). With currently 101 Contracting States,[68] the Convention can be viewed as one of the most successful family law instruments to be completed under the auspices of the Hague Conference on Private International Law.

Within the European Union, the operation of the 1980 Hague Abduction Convention has been modified by certain provisions of the Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast).[69] This EU instrument aims at creating even more ambitious rules on child abduction by imposing stricter obligations to assure the prompt return of a child.[70]

3.2.1. Locating the child and the abducting parent

Each Contracting State to the 1980 Convention must designate a so called 'Central Authority', which is responsible for the functioning of the Convention within

---

66 More generally, see Leenes, R.; De Conca, S., *Artificial Intelligence and Privacy – AI Enters the House Through the Cloud* in: Barfield *et al., op. cit.*, note 23, pp. 280-306.

67 Hague Convention on the Civil Aspects of International Child Abduction, 25 October 1980 ('1980 Hague Abduction Convention').

68 Hague Conference on Private International Law, *Status Table: Convention of 25 October 1980 on the Civil Aspects of International Child Abduction*, [https://www.hcch.net/en/instruments/conventions/status-table/?cid=24], Accessed 20 July 2023.

69 Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast) [2019] OJ L 178 ('Brussels IIa Recast Regulation').

70 See, generally, Trimmings, K., *Child Abduction within the European Union*, Hart Publishing, Oxford, 2013.

its territory.[71] In cases where, following the abduction, the whereabouts of the child are not known to the left-behind parent, the Central Authority is under the obligation to assist other competent authorities in locating the child.[72] This may be a situation where the abducting parent goes into hiding with the child, trying to prevent the child's return to the country of his/her habitual residence.[73] The question arises whether facial recognition software could be used to establish the whereabouts of such abducting parent and the child.

Not much has been written by academic commentators on the problem of locating children in international parental child abduction cases. The Hague Conference on Private International Law has emphasised on various occasions that 'Central Authorities, in seeking to locate children, should be able to obtain information from other governmental agencies and authorities and to communicate such information to interested authorities.'[74] The second Special Commission meeting of the Hague Conference to review the operation of the 1980 Convention encouraged Contracting States to include in their implementing legislation provisions giving wide powers to trial judges to locate a child even before the formal initiation of return proceedings. This should 'minimise delay in the initial location of the child, and thereby facilitate the initiation of return proceeding.'[75] It was also suggested that 'legislation may articulate powers for trial judges to direct third parties to disclose information about the location of children, or to issue a warrant for the authorities to make appropriate inquiries.'[76] Significantly, the Hague Conference Guide to Good Practice, Part 1 on Central Authorities states that 'Interpol can play a constructive and helpful role in locating abducted children.'[77] In some

---

71 1980 Hague Abduction Convention, *op. cit.* note 67, art 6. See also Hague Conference on Private International Law, *Guide to Good Practice under the Hague Convention of 25 October 1980 on the Civil Aspects of International Child Abduction: Part I – Central Authority Practice*, 2003, paras 4.10; 4.11; 5.24; and 5.25., [https://assets.hcch.net/docs/31fd0553-b7f2-4f34-92ba-f819f3649aff.pdf], Accessed 13 July 2023.

72 1980 Hague Abduction Convention, *op. cit.* note 67, art 7. Article 7(a) of the Convention imposes an obligation on Central Authorities to take appropriate steps to help locate a child.

73 E.g., *Re H. and Re S. and Another (Minors) (Abduction: Custody Rights)* [1991] 2 A. C. 476.

74 E.g., Hague Conference on Private International Law, *Conclusions and Recommendations of the Fourth Meeting of the Special Commission to Review the Operation of the Hague Convention of 25 October 1980 on the Civil Aspects of International Child Abduction*, 22–28 March 2001, para 1.9., [https://assets.hcch.net/upload/concl28sc4_e.pdf], Accessed 20 July 2023.

75 Hague Conference on Private International Law, *Report of the Second Special Commission Meeting to Review the Operation of the Hague Convention on the Civil Aspects of International Child Abduction*, 18-21 January 1993, [https://assets.hcch.net/docs/432981e4-238b-4ed4-a41e-bb239d5acdac.pdf], Accessed 10 June 2023.

76 *Ibid.*

77 Hague Conference on Private International Law, *op. cit.* note 71, para 4.10. See also Saskatchewan (Canada), International Child Abduction: Locating your Child, [https://www.saskatchewan.ca/residents/justice-crime-and-the-law/child-protection/international-child-abduction/locating-your-child],

countries, parental child abduction is a criminal offence; in others, it is not. The Guide to Good Practice, however, explains that 'it is not necessary to institute criminal proceedings in order to seek such help, which may be obtained on the basis of a missing persons report.'[78]

3.2.2. Should FRT be employed in locating the child and the abducting parent?

Having explored the concept of facial recognition in the EU context and the concerns surrounding the use of such applications, let us consider now whether such technologies could be used in the context of international parental child abduction. There is a strong argument for employing FRT in cases of abductions of children by strangers – acts that amount to a criminal offence under domestic criminal laws of all EU Member States.[79] This is reflected in the proposed AI Act, under which the use of FRT for the purpose of tracing a missing child represents one of the narrowly defined exceptions to the employment of remote biometric identification systems in publicly accessible spaces for law enforcement purposes.[80] However, when it comes to children who have been abducted by their own parent, the argument in favour of the employment of FRT in the child abduction context becomes weaker, partly because of the lack of uniformity among the Contracting States to the 1980 Hague Abduction Convention in criminalising such abductions.

The matter of blanket retention of biometric data for law enforcement purposes of persons not convicted of a crime was addressed by the ECtHR in *S. and Marper v. the UK*.[81] The Court pointed out that such retention may be particularly damaging when it comes to children, 'given their special situation and the importance of their development and integration into society.'[82] Moreover, when facial recognition is used to prevent, detect and investigate crime, it is difficult to see how this may justify the processing of facial images of children below the age of criminal responsibility.

Another concern arises in cases where the child has been missing for a protracted period of time. Ageing, i.e., the time between an image is taken and when it is

---

Accessed 20 July 2023. The latter source lists police, Interpol, the FBI and border authorities as organisations that can assist in recovery of abducted children in Saskatchewan.

78 Hague Conference on Private International Law, *op. cit.* note 71, para 4.10.

79 For analysis of the interface between criminal law and AI more generally see Pagallo, U.; Quattrocolo, S., *The Impact of AI on Criminal Law, and Its Twofold Procedures*, in: Barfield *et al., op. cit.*, note 23, pp. 385-409.

80 European Commission, *Shaping Europe's Digital Future: Regulatory Framework Proposal on Artificial Intelligence*, [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], Accessed 21 July 2023.

81 *S. and Marper v the United Kingdom*, Application No. 30562/04 and 30566/04, Judgment, 4 December 2008 [GC].

82 *Ibid.*, para 124.

compared, negatively affects the accuracy of facial recognition technologies. Scientific research does not allow for conclusions on the reliability of a match when more than five years have passed. The same holds true for facial images of older people if compared to images taken many years earlier, and therefore is applicable also to the abducting parent. Nevertheless, two points must be made in this respect: first, cases of abducting parents going into hi ding for extended periods of time are relatively rare; and, second, the likelihood of the left-behind securing the return of the child under the 1980 Hague Convention diminishes with time as, under Article 12, the court in the return proceedings will have to consider whether the child is now settled in his/her new environment, and, if that's the case, consider refusing the return application.

At the same time, in some cases, the impact of FRT on the best interests of the child may also be positive. Facial recognition systems can contribute to protecting the right of the child to preserve their identity. In parental child abduction cases, given the illegal nature of the removal or the retention of the child by the abducting parent, the child's right to identity is often violated as he/she is separated from the left-behind parent without any contact taking place. In line with the United Nations Convention on the Rights of the Child[83] (to which all EU Member States are Parties), where a child is deprived of some or all of the elements of their identity, States must provide appropriate assistance and protection, with a view to quickly re-establishing the identity of the child.

Against this background, it is submitted here that facial recognition systems used by the police and border guards may help trace missing and abducted children in parental child abduction cases. However, States must ensure that the systems are human rights compliant (see above section 3.1.3. Fundamental rights considerations), not only vis-à-vis the abducted child but also the abducting parent whose whereabouts the authorities are seeking to trace for the purposes of return proceedings under the 1980 Hague Convention.

4. CONCLUSION

As this article has demonstrated, digitalisation has impacted also the field of international family law. Cross-border assisted reproduction, which invariably involves the use of the internet and other forms of digital technologies to connect the parties, is one example of such interaction. In this respect, cross-border surrogacy arrangements in particular demonstrate the legal complexities that often result from

[83] UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, Vol. 1577, p. 3, art 8.

such arrangements. Another example of the interface between international family law and digital technologies is the potential utility of AI-powered FRTs in the process of locating children and abducting parents in international parental child abduction cases under the 1980 Hague Abduction Convention. Although this is considered feasible, national legislators are urged to exercise caution to ensure that relevant legal frameworks guarantee protection of fundamental rights of the child and the abducting parent.

REFERENCES

BOOKS AND ARTICLES

1. Adjabi, I., et al*, Past, Present, and Future of Face Recognition: A Review*, Electronics, Vol. 9, No. 8, 2020, p. 1188
2. Barfield, W.; Pagallo, U. (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Cheltenham, 2018
3. Bergamini, E.; Ragni, C., *Fundamental Rights and Best Interests of the Child in Transnational Families*, Intersentia, Cambridge, 2019
4. Cheung, A.; Chen, Y., *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, Law & Social Inquiry, Vol. 47, No. 4, 2022, pp. 1137-1171
5. Cohen, G., *Patients with Passports*, Oxford University Press, Oxford, 2015
6. Dale, B.; Elder, K., *In Vitro Fertilisation*, Cambridge University Press, Cambridge, 1997
7. Deech, R., *Reproductive Tourism in Europe: Infertility and Human Rights*, Global Governance, Vol. 9, No. 4, 2003, pp. 425–432
8. Hird Chung, L., *Free Trade in Human Reproductive Cells: A Solution to Procreative Tourism and the Unregulated Internet*, Minnesota Journal of International Law, Vol. 15, 2006, pp. 263-296
9. Meniru, G.; Brinsden P.; Craft, I., *A Handbook of Intrauterine Insemination*, Cambridge University Press, Cambridge, 1997
10. Obasogie, O.K.; Darnovsky, M. (eds.), *Beyond Bioethics: Toward a New Biopolitics*, 2018.
11. O'Flaherty, M., *Facial Recognition Technology and Fundamental Rights*, European Data Protection Law Review, Vol. 6, 2020, pp. 170-173
12. Pennings, G., *Legal Harmonization and Reproductive Tourism in Europe*, Reproductive Health Matters, Vol. 13, No. 25, 2005, pp. 120–128
13. Pennings, G., *Reproductive Tourism as Moral Pluralism in Motion*, Journal of Medical Ethics, Vol. 28, No. 6, 2002, pp. 337–341
14. Sheriff, D.S. (ed.), *Infertility, Assisted Reproductive Technologies and Hormone Essays*, IntechOpen, London, 2019
15. Simopoulou, M. *et.al.*, *Discarding IVF Embryos: Reporting on Global Practices*, Journal of Assisted Reproduction and Genetics, Vol. 36, 2019, pp. 2447–2457
16. Speier, A., *Fertility Holidays: IVF Tourism and the Reproduction of Whiteness*, New York University Press, New York, 2016

17. Storrow, R., *Quests for Conception: Fertility Tourists, Globalization and Feminist Legal Theory*, Hastings Law Journal, Vol. 57, 2006, pp. 295-330
18. Swink D.; Reich, B., *Outsourcing Reproduction: Embryos and Surrogacy Services in the CyberProcreation Era*, Ethics and Business Law Faculty Publications, Vol. 14, 2011, pp. 1-62
19. Deonandan, R.; Green, S.; van Beinum, A., *Ethical Concerns for Maternal Surrogacy and Reproductive Tourism*, Journal of Medical Ethics, Vol. 38, 2012, pp. 742-745
20. Trimmings, K., *Child Abduction within the European Union*, Hart Publishing, Oxford, 2013
21. Trimmings, K.; Shakargy, S.; Achmad C., *Research Handbook on Surrogacy and the Law,* Edward Elgar Publishing, Cheltenham, 2024 (forthcoming)
22. Waelen, A., *The Struggle for Recognition in the Age of Facial Recognition Technology*, AI Ethics, Vol. 3, 2023, pp. 215–222
23. Veale, M.; Zuiderveen Borgesius, F., *Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, Computer Law Review International, Vol. 22, No. 4, 2021, pp. 97-112
24. Vida, P., *Surrogate Tourism and Reproductive Rights*, Hypatia, Vol. 28, No. 2, 2013, pp. 274–289

ECHR

1. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5
2. *Labassee v France*, Application No. 65941/11, 26 June 2014
3. *Mennesson v France*, Application No. 65192/11, ECHR 2014 (extracts)
4. *S. and Marper v the United Kingdom*, Application No. 30562/04 and 30566/04, Judgment, 4 December 2008 [GC]

EU LAW

1. Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast) [2019] OJ L 178
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
3. 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

INTERNATIONAL CONVENTIONS

1. Hague Convention on the Civil Aspects of International Child Abduction, 25 October 1980

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. *Re A* [2014] EWFC 55
2. *Re H. and Re S. and Another (Minors) (Abduction: Custody Rights)* [1991] 2 A. C. 476
3. *Re Z (A Child)* [2016] EWFC 34
4. *Re T (a child) (surrogacy: residence order)* [2011] EWHC 33 (Fam)
5. *Z and another v C and another* [2011] EWHC 3181 (Fam)

UNITED NATIONS SOURCES

1. UN Special Rapporteur on the Sale of the Child, *Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material*, A/74/162, 2019, [https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/216/49/PDF/N1921649.pdf?OpenElement], Accessed 20 July 2023

WEBSITE REFERENCES

1. Castelluccia, C.; and Le Métayer Inria, D., *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*, Centre for Data Ethics and Innovation, 2020, [https://inria.hal.science/hal-02480647/document], Accessed 14 April 2023
2. Council of Europe Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, 2019, [https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64], Accessed 20 July 2023
3. Crumpler W., *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, 2020, [https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it], Accessed 20 July 2023
4. European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, 2019, [https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law], Accessed 12 March 2023
5. European Commission, *Regulatory Framework Proposal on Artificial Intelligence*, [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], Accessed 13 May 2023
6. European Commission, *Shaping Europe's Digital Future: Regulatory Framework Proposal on Artificial Intelligence*, [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], Accessed 21 July 2023
7. European Commission, *Study on the Use of Innovative Technologies in the Justice Field*, 2020, [https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1], Accessed 20 July 2023
8. European Court of Human Rights, Press Unit, *Factsheet – Gestational Surrogacy*, 2022, [https://www.echr.coe.int/Documents/FS_Surrogacy_eng.pdf], Accessed 19 July 2023
9. European Digital Rights (EDRi), *Will the European Parliament Stand Up for Our Rights by Prohibiting Biometric Mass Surveillance in the AI Act?*, 2022, [https://edri.org/our-work/

will-the-european-parliament-stand-up-for-our-rights-by-prohibiting-biometric-mass-surveillance-in-the-ai-act/], Accessed 10 April 2023

10. European Parliament, Regulating Facial Recognition in the EU, 2021, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf], Accessed 20 July 2023
11. French Data Protection Agency (CNIL), *Privacy Impact Assessment (PIA)*, [https://www.cnil.fr/en/privacy-impact-assessment-pia], Accessed 20 July 2023
12. Goldenfein, J., *Facial Recognition is Only the Beginning*, 2020, [https://www.publicbooks.org/facial-recognition-is-only-the-beginning/], Accessed 12 April 2023
13. Hague Conference on Private International Law, *Conclusions and Recommendations of the Fourth Meeting of the Special Commission to Review the Operation of the Hague Convention of 25 October 1980 on the Civil Aspects of International Child Abduction*, 22–28 March 2001, [https://assets.hcch.net/upload/concl28sc4_e.pdf], Accessed 20 July 2023
14. Hague Conference on Private International Law, *Guide to Good Practice under the Hague Convention of 25 October 1980 on the Civil Aspects of International Child Abduction: Part I – Central Authority Practice*, 2003, [https://assets.hcch.net/docs/31fd0553-b7f2-4f34-92baf819f3649aff.pdf], Accessed 13 July 2023
15. Hague Conference on Private International Law, Parentage / Surrogacy Project, 2011-to date, [https://www.hcch.net/en/projects/legislative-projects/parentage-surrogacy], Accessed 20 July 2023
16. Hague Conference on Private International Law, *Report of the Second Special Commission Meeting to Review the Operation of the Hague Convention on the Civil Aspects of International Child Abduction*, 18-21 January 1993, [https://assets.hcch.net/docs/432981e4-238b-4ed4-a41e-bb239d5acdac.pdf], Accessed 10 June 2023
17. Hague Conference on Private International Law, *Status Table: Convention of 25 October 1980 on the Civil Aspects of International Child Abduction*, [https://www.hcch.net/en/instruments/conventions/status-table/?cid=24], Accessed 20 July 2023
18. Introna, L.; and Nissenbaum, H., *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030, [https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf], Accessed 10 May 2023
19. Politico, *Europe Edges Closer to a Ban on Facial Recognition*, 2022, [https://www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/#:~:text=And%20while%20the%20European%20Commission,locating%20armed%20and%20dangerous%20criminals], Accessed 19 June 2023
20. Saskatchewan (Canada), International Child Abduction: Locating your Child, [https://www.saskatchewan.ca/residents/justice-crime-and-the-law/child-protection/international-child-abduction/locating-your-child], Accessed 20 July 2023
21. Schneier, B., *We Are Banning Facial Recognition. We're Missing the Point*, New York Times, 20 January 2020, [https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html], Accessed 10 April 2023
22. Ville de Nice, *Rapport: Experimentation Reconnaissance Faciale*, 2019, [https://s3.documentcloud.org/documents/6350838/Bilan-Reconnaissance-Faciale.pdf], Accessed 15 April 2023

UDK 347.67:004]:341.9
Review article

MANAGING CROSS-BORDER "DIGITAL SUCCESSION" IN THE DIGITAL ERA: PRELIMINARY REMARKS ON THE NEW CHALLENGES FOR THE CURRENT LEGAL FRAMEWORK*

Ilaria Viarengo, PhD, Full Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio, 7, 20 122 Milan, Italy
ilaria.viarengo@unimi.it

Jacopo Re, PhD, Associate Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio, 7, 20 122 Milan, Italy
jacopo.re@unimi.it

ABSTRACT

This paper aims to answer to a rather common question: what happen to our digital estate when we die? To do so, after analysing the composition of a digital estate, the paper will determine, firstly, the legal framework applicable to a cross-border succession to a digital estate. It will then investigate: (i) which assets are transferable upon death and to what extent; (ii) under what conditions heirs have access to the deceased's accounts; and (iii) which interests on the digital content created by the deceased are protected and how. The analysis will be conducted through the lens of the current private international law framework in force in EU Member States, in order to formulate some preliminary remarks on its adequacy to manage this new succession phenomenon and the issues it raises.

Keywords*: Digital estate, Characterisation, Cross-border successions, European Succession Regulation, Personality rights*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. The present contribution is the result of common research and reflection of both authors and was prepared in their mutual collaboration. However, strictly regarding the process of drafting, it is specified for academic evaluation purposes that paragraphs 1 and 2 are to be attributed to Prof. Ilaria Viarengo, whilst paragraphs 3 and 4 are to be attributed to Prof. Jacopo Re; paragraph 5 is to be attributed to both authors.

1. INTRODUCTION

It is a common experience that, in today world, Internet is a constant reality and has given birth to a person's digital life side by side his/her real life, creating new phenomena and situations that seek to find their legal regulations, whether it is an *ad hoc* one or an adaptation of existing rules. Once data are created or uploaded in the cloud, they can live in the virtual world regardless of their creator's natural life.

On the other hand, succession law, a branch of law perceived as highly resistant to changes and innovations, traces its roots in the traditions and in the values of any given society. As it is well-known, it is aimed at solving, at a legal level, an ancestral anthropological problem:[1] that of the fate of a person's estate at the time of his/her death, in order to avoid, to the greatest extent, any legal uncertainty.

On this premises, this paper aims to formulate some preliminary remarks on whether the current legal framework in force in EU Member States for cross-border successions is adequate to manage the succession to digital estate and the issues it raises.

2. SETTING THE SCENE

Before addressing the private international law regime of digital heritage,[2] three preliminary caveats have to be considered.

The first one deals with the notions of digital inheritance/digital assets. These notions are becoming more widespread and relevant in today societies, where digital devices and Internet play a dominant role in our lives. Everyday, in the cloud, we leave digital footprints or traces. These might be worth a lot from different points of view: economical (e.g. domain names), personal and emotional (e.g. digital picture or videos, data in social media accounts) or due to the efforts of time and resources in creating it (e.g. youtube videos).[3]

---

1 Marino, M., *Mercato digitale e Sistema delle successioni* mortis causa, Edizioni Scientifiche Italiane, Napoli, 2022, p. 11.

2 On the matter, see, Merchán Murillo, A., *La sucesión digital internacional y el Reglamento sucesorio europeo 650/2012*, Anuario español de derecho internacional privado, Vol. 21, 2021, pp. 327-357.

3 Maeschaelck, B., *Digital Inheritance in Belgium*, European Journal of Consumer and Market Law, Vol. 4, No. 1, 2018, pp. 37-41; Mackenrodt, M.-O., *Digital Inheritance in Germany*, European Journal of Consumer and Market Law, Vol. 4, No. 1, 2018, pp. 41-48. For the purpose of this paper, digital asset is defined as "an electronic record which is capable of being subject to control". On the matter, see Principle 2(2) of the Draft UNIDROIT Principles on Digital Assets and Private Law, available at [https://www.unidroit.org/wp-content/uploads/2023/01/Draft-Principles-and-Commentary-Public-Consultation.pdf],, Accessed 5 July 2023.

Furthermore, a digital estate is comprised of assets and goods with different features. Some goods are the online version of traditional ones, such as bank and investments accounts. Other goods are created online, like digital paying instruments who have deposit account functions (Paypal). Again, there are general accounts used for a number of services or as a gateway to a person's virtual life (Google and Apple accounts for Google and Apple services), or single and different social media accounts, being them personal or professional ones (e.g. Instagram and Facebook, for the first group, or Linkedin, for the latter) or having a combination of both aspects (like Youtube, especially in the event of a person making a living out the video uploaded). Moreover, a digital heritage may be comprised of in-cloud storage (Dropbox, Google drive) or online entertainment services (e.g. Spotify or Netflix), as well as crypto assets.[4] The variety of types of assets that form a person's digital estate, each with different economic or personal value, makes it clear from the outset that a uniform solution as to their transferability upon death might be difficult to reach.

The second preliminary warning deals with the problem on how the aforementioned estate affects the nature, national or international, of a succession. It is clear that digital estate is, by its very nature, ubiquitous and escapes and transcends the borders of a single State. So, a question arises on whether a person's digital life, in itself, makes his/her succession cross-border, thus subject the private international law regime of cross-border succession.[5]

In this regard, it might be noted that, if the question is to be answered in the affirmative, given the widespread reach of the phenomenon, every succession to estate that are comprised of digital goods or services should be characterised as cross-border, even if, in the real world, the deceased's estate and his/her personal connections are located in a single State. This result would lead to debasement of the *raison d'être* of private international law rules themselves, as a system of rules

---

4 See, for a similar classification, Merchán Murillo, *op. cit.*, note 2, p. 351 f. It is worth noting that, recently (31 May 2023), the European Union legislator has adopted Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40. According to Art 3(1)(5) of Regulation No 2023/1114, crypto-assets are defined as "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology". On this Regulation see Villata, F.C., *Il regolamento (UE) 2023/114 relativo ai mercati delle cripto-attività: prime note con un occhio al diritto internazionale privato*, Rivista di diritto internazionale privato e processuale, Vol. 59, No. 3, 2023, forthcoming.

5 On the private international law rules and techniques in succession matters see, for all, Bonomi, A., *Successions internationales: conflits de lois et de juridictions*, Recueil des Cours, Vol. 350, 2011, pp. 71-418.

governing private relationships that have points of connection with several States, geographically definable.[6]

So, at a first appraisal, entering into digital contracts – that creates digital goods and services and that may be characterised, themselves, as cross-border – do not internationalise a domestic succession. In this direction, it does not seem improper to consider the digital estate to be located by the deceased in order to assess the international character of a succession.[7]

The previous findings leave the floor open to the third and last problem. Once a person's succession is characterised as international – for having connections, in the real world, with at least two different States – it might be asked if the solutions provided by the private international rules of a legal system are applicable to the digital estate too.

From the perspective of European Union's Member States, an affirmative answer seems to be favourable, in the light of the relevant legal framework: this consists, on the one hand, of the European Succession Regulation,[8] and, on the other hand, of the General Data Protection Regulation.[9]

---

6 On the object and functions of private international law see Mosconi, F., *Oggetto e funzione*, in: Baratta, R. (a cura di), Diritto internazionale privato, Giuffrè, Milano, 2010, pp. 262-273; Rühl, G., *Private international law, foundations*, in: Basedow, J., Rühl, G., Ferrari, F., de Miguel Asensio, P. (eds.), Encyclopedia of Private International Law, Edward Elgar Publishing, Cheltenham-Northampton, 2017, pp. 1380-1390. On the impact of Internet on private international law see de Miguel Asensio, P., *Conflict of Laws and the Internet*, Edward Elgar Publishing, Cheltenham-Northampton, 2020.

7 *Mutatis mutandis*, a similar reasoning can be glimpsed in Court of Justice of the European Union, Joined Cases C509/09 and C161/10, *eDate Advertising GmbH*, [2011] ECR I-10269, par. 48-49, where, in a claim over infringement of personality rights, the Court of Justice gave jurisdiction to the Court of the place where the alleged victim has his centre of interests – i.e., the place of his habitual residence – since it is the closest one to the place where the harmful event occurred. Furthermore, in most jurisdictions that adopt the system of scission – which differentiate between movables and immovables property – a not dissimilar reasoning underlies the rule that the succession to movables is governed by the personal law of the deceased, on the premise that *mobilia persona sequuntur*. See, Grahl-Madsen, A., *Conflict between the Principle of Unitary Succession and the System of Scission*, The International and Comparative Law Quarterly, Vol. 28, 1979, p. 598 f.

8 Regulation (EU) No 650/2012 of the European Parliament and of the Council on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L201/107.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council 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), [2016] OJ L119/1. On the connection between privacy and digital death see Harbinja, E., *Digital Death, Digital Assets and Post-Mortem Privacy*, Edinburgh University Press, Edinburgh, 2023.

As it is well known, Regulation No 650/2012 adopts the unitary approach.[10] According to Recital No 42, Arts 4 and 21, the competent Court of the Member State where the deceased has his/her habitual residence at the time of his/her death and the law of the State of his/her habitual residence at the time of the death govern the succession as a whole. Moreover, the reach of the Succession Regulation, is defined, in negative, by the exclusions listed in Art 1(2) and, in positive, by the scope of the applicable law, as provided in art Art 23. Although those Articles do not consider expressly digital estate, the very nature of the unitary approach – which determines the competent judicial authority and the applicable law regardless of the nature of the estate, being it movable, immovable, and, it might be added, digital – stands for the application of private international rules to the digital estate as well.

From the perspective of the protection of personal data, relevant in the case of digital heritage, it is worth noting that Regulation (EU) 2016/769 does not apply to the personal data of deceased persons. However, as stated in Recital No 27 of the Regulation, Member State may adopt and implement national rules on the matter.[11]

After having assessed that, in principle, private international law rules are applicable to a cross-border succession in the deceased digital estate, the investigation will be conducted along the following lines.

On the one hand, proprietary rights in digital goods and services have to be differentiate from personality rights, since only the former fall within the scope of succession law. This scrutiny is quite complex with regard to digital goods, as the proprietary element of digital data is, often, intimately connected with the identity of the person. However, it might be sensible to point out that some digital assets have a (predominant) proprietary nature: this is true for online bank/investment accounts; digital payment instruments and in cloud storage. For other assets, such as general accounts (Google account, Apple ID) and social media accounts, the two sides of the problem are so intertwined that it might be difficult to rest on the usual division between proprietary and personal rights in order to assess their transmissibility upon death.[12]

---

10 On the difference between the unitary and scission approach, see Bonomi, *op. cit.*, note 5, pp.99-133.

11 See, for example, Art 63 of the French Law 7 October 2016 No 2016-1321 for a Digital Republic (pour une République numérique), Official Journal No 235/2016; Art 2-terdecies of the Italian Legislative Decree 30 June 2003 No 196, Personal Data Protection Code (Codice in materia di protezione dei dati personali), Official Journal No 174/2003, as modified by the Legislative Decree 10 August 2018 No 101, Official Journal No 205/2018.

12 Marino, M., *La successione digitale*, Osservatorio del diritto civile e commerciale, No. 1, 2018, pp. 167-204.

On the other hand, the digital estate of the deceased is created by a network of contracts – each of which is governed by its own applicable law and its own general terms and conditions – that, independently, might influence the transmissibility of the contract upon death.

Lastly, the succession in digital heritage can be intended both as succession in the accounts, or as protected interests on the digital content created by the deceased.

3. SUCCESSION IN DIGITAL PROPERTY AND IN THE ACCOUNTS

When digital assets embed proprietary rights or have an intrinsic economic value, these are, *prima facie*, transferrable upon death. To uphold this solution, a general principle of law can assist the interpreter. The principle of functional equivalence – according to which digital/intangible estate is equivalent to tangible estate, so that the former should not be discriminated against in relation to any other type of manifestation – can place digital estate within the rules regulating succession as a whole.[13] From a comparative perspective, many legal systems regulate the transferability upon death of digital assets with economic value as inheritance rights.[14] Thus, the widespread universality principle of substantive law, coupled with the unitary approach of the European Succession Regulation, contribute to confirm the aforementioned statement.

Therefore, in a cross-border situation, considering that the European private international regime regulates digital assets too, it is sensible to affirm that the law applicable to the deceased's succession – being it, the law of his/her habitual residence at the time of death, as per Art 21 of the European Succession regulation,[15] or the law of his/her nationality, in case of a valid *professio iuris* under Art 22 of the Regulation[16] – will determine the succession on his/her digital estate, when the

---

13 Merchán Murillo, *op. cit.*, note 2, p. 352.

14 In Belgian law, see Maeschaelck, *op. cit.*, note 3, p. 38; in German law, see Mackenrodt, *op. cit.*, note 3, p. 42; in the law of the Netherland, see Berlee, A., *Digital Inheritance in the Netherlands*, European Journal of Consumer and Market Law, Vol. 3, No. 6, 2017, pp. 256-260; in the law of the United Kingdom (and its legal systems), see Harbinja E., *Digital Inheritance in the United Kingdom*, European Journal of Consumer and Market Law, Vol. 3, No. 6, 2017, pp. 253-256. See, moreover, Fras, M., *Succession of digital goods. A comparative legal study*, Review of European and Comparative Law, Vol. 47, No. 4, 2021, pp. 67-81.

15 See, Re, J., *Where Did They Live? Habitual Residence in the Succession Regulation*, Rivista di diritto internazionale privato e processuale, Vol. 54, No. 4, 2018, pp. 978-1009; Pazdan, M., Zachariasiewicz, M., *The EU succession regulation: achievements, ambiguities, and challenges for the future*, Journal of Private International Law, Vol. 17, No. 1, 2021, pp. 74-113.

16 See, Viarengo, I., *Planning Cross-Border Successions: the Professio Juris in the Succession Regulation*, Rivista di diritto internazionale privato e processuale, Vol. 56, No. 3, 2020, pp. 559-582.

assets comprised embed proprietary rights or have an intrinsic economic value. As a result, succession in online bank/investment accounts; digital payment instruments and in cloud storage would follow the well-established path laid down by succession rules.

From another perspective, since digital assets are usually created by contracts, a limitation on their transmissibility *mortis causa* might derive from the law applicable to the contract or from their general terms and conditions. This might be relevant for general accounts, such as Google account or Apple ID, and social media accounts, assets in which the digital estate includes both proprietary and personal rights; hence the problem of devolution, which traditionally excludes the latter.

For these assets, the shrewdest legal scholarship, as well as the earliest national case-law, points to a different treatment of the problem of the succession to the account, on the one hand, and that of the protection of interests on the digital content created by the deceased.[17]

With regards to the first problem, three different regulatory schemes seem to emerge for the early and available practice.[18] The first one, the proprietary approach, is based on the application of the universality principle, combined with the principle of equivalence. In line with the traditional approach and the concept of the succession as *universitas*, this approach emphasises the proprietary or strictly inheritance profile, by virtue of which the heir, succeeding in all the active and passive relationships of the *de cuius*, must also succeed in the contractual relationship already concluded between the latter and the service provider.

The second one, the personalistic approach, admits the extended enforcement of some aspects of the deceased's digital personality, but does not allow for the succession in the ownership of the account.

The third (and last) one, the voluntarist approach, confers importance and effectiveness to the general terms and conditions of the contract signed by the user at the time he/she opened the account (and to the following modifications): in this context, it is not rare that the digital service provider includes either a non-transferability agreement of the data to the heirs or the possibility for the user to designate a so-called "heir contact" – to be called in the event that the user's account is not active for a certain period of time – that will have access to the content indicated by the user and with the power vested by him.

---

17 See Marino, *op. cit.*, note 12, pp. 179-189; Fras., *op. cit.*, note 14, pp. 70-71.

18 See, Spangaro, A., *La successione digitale: la permanenza* post mortem *di aspetti della personalità*, Giurisprudenza italiana, No. 6, 2022, pp. 1363-1370.

The three approaches may appear, at a first glance, mutually exclusive. However, it might be argued that they can be combined in order to manage smoothly different situations.

The starting point are the rules of the *lex successionis* governing the succession to the contractual obligation of the deceased. If, according to that law, heirs succeed to the deceased in the contractual positions held by him, they are entitled, in principle, to succeed in the account, unless, by way of exception, the nature of the contract itself, or other rules of the legal system, do not allow for its transferability upon death.[19]

However, due attention has to be payed to the general terms and conditions of the contract concluded between the deceased and the service provider and to the law applicable to that contract. Indeed, the general terms and conditions of the service provider can qualify the contractual relationship as granting limited, non-exclusive, non-transferable right,[20] or can state expressly the termination of the account upon the user's death.[21]

In these cases, even if the law applicable to the succession provides for the transferability upon death of contractual obligations, the will of the parties as to the nature of the rights and their transferability, as agreed in the general terms and conditions of the contract signed by the user, prevails. Therefore, when the contractual framework states the termination of the contract upon the user's death or qualifies those rights as non-transferable by way of succession, those digital assets – and the ownership of the account – do not fall into succession.[22]

Conversely, when the general terms and conditions of a given digital asset do not consider the death of the user, and no exception is provided for in the *lex succes-*

---

19 For example, in Italian substantive law, the general rule is for the succession in the contracts concluded by the deceased, except for those characterised by *intuitus personae*. See, Palazzo, A., Sassi, A., *Trattato della successione e dei negozi successori*, Vol. 1, *Categorie e specie della successione*, Utet, Torino, 2012, p. 590. Moreover, in a comparative perspective see Fras., *op. cit.*, note 14, p. 77 ff.

20 See Netflix Terms of Use No 4.2, available at [https://help.netflix.com/en/legal/termsofuse], Accessed 5 July 2023, according to which "During your Netflix membership we grant you a limited, non-exclusive, non-transferable right to access the Netflix service and Netflix content. Except for the foregoing, no right, title or interest shall be transferred to you".

21 See iCloud condition No IV.D, available at [https://www.apple.com/legal/internet-services/icloud/], Accessed 5 July 2023, according to which "Except as allowed under Digital Legacy and unless otherwise required by law, you agree that your Account is non-transferable and that any rights to your Apple ID or content within your Account terminate upon your death. Upon receipt of a copy of a death certificate your Account may be terminated and all content within your Account deleted".

22 Needless to say, the contractual aspects of the relationship between the user and the provider are governed, as to the applicable law, by Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

sionis, the combined effect of the universality principle and unitary approach leads to the transferability upon death of the digital asset and of the account. This result seems justified – combining the proprietary approach with the voluntarist one – both by the aforementioned principle of functional equivalence and, lacking any *ad hoc* rule for digital asset, by way of analogy.

The lack of any express provision on the non-transferability upon death of the ownership of the account has been evaluated by the German Federal Court, in its well-known judgment of 12 July 2018.[23] The judgment settled a dispute between the parents (and heirs) of a 15 years old girl, who died in a tram accident, and Facebook. The parents wanted to obtain access to the user account of their deceased daughter and to the messages stored within, in order to clarify the circumstances of her death, and to learn whether she intended to commit suicide or if she was victim of a tragic accident. However, Facebook denied access to that information. While the first instance Court granted access to the Facebook account of the deceased daughter, on appeal, the second instance Court rejected the claim of the parents, on the ground that allowing access to the account would be contrary to the provisions protecting the secrecy of telecommunications.[24]

The Bundesgerichtshof characterised the plaintiff's claim as hereditary. Although the dispute raised serious questions on *post mortem* protection of personal rights and personal data, secrecy of correspondence, and protection of the personal interests of partners in communication, the German Court found that in the "contract between the deceased and the portal's administrator the possibility was not excluded of the heirs entering into the rights and obligations of the former", therefore allowing access to the deceased's account.[25]

Thus, in the light of the above, in a cross-border situation, it might be advanced that it is for the *lex successionis* to regulate the succession to digital estate not only when the assets have proprietary aspects or an intrinsic economic value, but also when the general terms and condition of the contracts creating them do not exclude their transferability upon death.

From another perspective, it should not be overlooked that the enjoyment and enforcement of such rights may not be easy if the law of the country in which the digital service provider is located does not permit the transfer of such assets and rights *mortis causa*.

---

23 Bundesgerichtshof, 12 July 2018 III ZR 183/17, NJW, 2018, pp. 3178-3187.

24 Mackenrodt, *op. cit.*, note 3, p. 42.

25 Fras., *op. cit.*, note 14, p. 73.

Lastly, should a dispute arise between the deceased's heirs and the digital provider, given that the European Succession Regulation applies to digital assets too, the competent Court will be determined in accordance with Arts 4-11 of the Regulation.[26] In this respect, the Regulation sets up an autonomous and sufficient system of rules, suitable for preventing positive conflicts of jurisdiction, structured along two precise lines. On the one hand, the Regulation seeks to identify a single Court with jurisdiction for all disputes arising from a given succession. On the other hand, it provides for mechanisms enabling, as far as possible, jurisdiction to be conferred on the Court of a Member State whose law governs the succession. The general head of jurisdiction (Art 4) is the deceased's last habitual residence at the time of his/her death. However, should the deceased have chosen his/her *lex patriae* as the law regulating his/her succession, and that law is the law of a Member States, Arts 5-9 provides various techniques to restore the *Gleichlauf* between *jus* and *forum*. Subsidiary jurisdiction (Art 10), in the case the deceased's last habitual residence was not located in a Member State, rests on the Courts of a Member State in which assets of the estate are located in so far as the deceased was a citizen of that State at the time of the death, or, failing that, the deceased had his previous habitual residence in that Member State, provided that, at the time the Court is seised, a period of not more than five years has elapsed since that habitual residence changed. A provision on *forum necessitatis* completes the Regulation jurisdictional rules (Art 11).

4. PROTECTED INTERESTS ON THE DIGITAL CONTENT CREATED BY THE DECEASED AND THE ROLE OF THE DIGITAL HEIR

When the general terms and conditions of the digital asset do not allow the succession in the account, there might be, nevertheless, protected interests of the heirs to access to the digital contents created by the deceased and posted or stored in the account.

On the one hand, heirs might have a right to the intellectual property rights on the deceased's intellectual works conveyed by the digital medium (such as app, photos, videos, software, domain name) and their related economic use (e.g. videos on Youtube having high views rates). Given the scope of succession rules – that is to avoid, to the greatest extent, any legal uncertainty to the fate of a person's

[26] On the jurisdictional rules of the European Succession regulation see, for all, Queirolo, I., *Jurisdiction in succession matters: General rules and choice of court*, in: Bariatti, S.; Viarengo, I.; Villata, F.C. (eds.), EU Cross-Border Succession Law, Edward Elgar Publishing, Cheltenham-Northampton, 2022, pp. 219-243.

estate – it has been argued that it would be contrary to a rule of public policy for the digital server provider not to grant access to those assets.[27] Therefore, it would be for the *lex successionis* to regulate the transferability *mortis causa* of these assets.

On the other hand, the personalistic approach might have some room when the interest of the heirs to access to the digital data is not justified by a proprietary or economic nature of the asset, but by other reasons.

As already mentioned, Regulation No 2016/769 does not apply to the personal data of deceased persons, but, according to Recital No 27, Member State may adopt and implement national rules on the matter. In Italy, for example, Art 2-*ter-decies* of Legislative Decree No 196/2003, as modified by the Legislative Decree No. 101/2018, allows anyone who has an interest of his own, or acts to protect the deceased, as his/her representative, or for family reasons worthy of protection, to exercise the rights conferred by Arts 15-22 of the GDPR. On this ground, some Italian judges granted access to the digital content stored in a general account (i.e., iCloud).[28]

In a cross-border situation, a problem of characterisation of these remedies might arise. Since Art 3(1)(a) of the European Succession Regulation defines succession as "succession to the estate of a deceased person and covers all forms of transfer of assets, rights and obligations by reason of death, whether by way of a voluntary transfer under a disposition of property upon death or a transfer through intestate succession", and since the access to digital content non having proprietary or economic nature cannot be granted always by their transferability upon death, due to the limitation provided for in the general terms and conditions, a characterisation as matter related to a succession seems to be excluded.

Indeed, these remedies find their private international law regulation both on other EU Regulations and on national rules. Applying the autonomous notion of civil and commercial matters, it might be argued that Regulation (EU) No 1215/2012 is applicable for claims arising out of an infringement of personality rights.[29] In

---

27 Marino, *op. cit.*, note 12, pp. 182-183.

28 The interest of the family members might be of different nature: the will to celebrate the life of the deceased, or the desire to keep family memories, or, again, the urge to know the circumstances of the *de cuius*' death. In these cases, against Apple's objection to allow access to the deceased's account, Italian Courts granted this right to family members on the basis of the national implementation of GDPR rules. See: Tribunale di Milano, 10 February 2021, Giurisprudenza italiana, 2022, No. 6, 1363; Tribunale di Bologna, 25 November 2021, De jure, Tribunale di Roma, 10 February 2022. On the last two judgments see, Maniaci, A., d'Arminio Monforte, A., *"Eredità digitale" e accesso ai dati personali del defunto*, Diritto di Internet, No. 3, 2022, pp. 561-573.

29 See, Kuipers, J.-J., *Personality rights*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), Encyclopedia of Private International Law, Edward Elgar Publishing, Cheltenham-Northampton,

this perspective, both Art 4 and Art 7(2) can serve as grounds for jurisdiction. However, should the defendant be not domiciled in a Member State, national rules on jurisdiction apply. As per Art 1(2)(g) of Regulation No 864/2007, Rome II Regulation does not apply to "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation". Therefore, it is for the national private international law rules on personality rights to provide for the applicable law. Eventually, recognition and enforcement of judgments delivered by any Court of a Member State will be subject to Chapter III of Regulation No 1215/2012; conversely, judgments for third Countries will be recognised and enforced according to national rules.

From a different perspective, the family members' interest in accessing to the digital content might find two limits. On the one hand, the deceased might have expressly prohibited the exercise of aforementioned rights during his/her life. On the other hand, he/she might have designated a "heir contact" to whom the digital service provider has to grant access to the account.

In this perspective, it is not uncommon to find – in the general terms and conditions of use of Internet services – a contractual clause by which the user can indicate the "heir contact", who will have access to the contents of the account and can dispose of them.[30] In a cross-border situation, this clause might be qualifiable as a *post-mortem* mandate. Should the designated heir accept the mandate, it is sensible to characterise the relationship as having a contractual nature, therefore falling into the scope of Regulation No 1215/2012 and Regulation (EC) No 593/2008, that will provide for the relevant private international law regime.

2017, pp. 1351-1359. See also Regulation (EU) No 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1. Moreover, since Regulation No 2016/769 does not apply to the personal data of deceased persons, it follows that the rule provided in Art 79(2) of the Regulation can not serve as a ground for jurisdiction. On Art 79(2) of Regulation No 2016/769 see de Miguel Asensio, P., *op. cit.*, note 7, pp. 152-162.

30 See iCloud condition No II.L, available at [https://www.apple.com/legal/internet-services/icloud/], Accessed 5 July 2023, according to which "With Digital Legacy, you can choose to add one or more contacts to access and download certain data in your account after your death. If your designated contacts provide proof of death to Apple and have the required key, they will automatically obtain access to that certain account data and activation lock will be removed from all your devices". In the United States, a first regulation of the rights and duties of the "heir contact" has been provided for by the Uniform Law Commission with the Fiduciary Access to Digital Assets Act, Revised of 2015. Its status and implementation in State law are available at [https://www.uniformlaws.org/committees/community-home?communitykey=f7237fc4-74c2-4728-81c6-b39a91ecdf22], Accessed 5 July 2023. On the Fiduciary Access to Digital Assets Act, Revised see, among others, Woodman, F.L., *Fiduciary Access to Digital Assets: A Review of the Uniform Law Conference of Canada's Proposed Uniform Act and Comparable American Model Legislation*, Canadian Journal of Law and Technology, Vol. 15, No. 2, 2012, pp. 193-227.

5. CLOSING REMARKS

The digital era poses new challenges to the traditional succession rules with regards to the transferability upon death of the digital estate. As it has been outlined, the first challenge is to clearly differentiate the digital assets having a proprietary and economic value – which, *prima facie*, fall into the scope of succession rules – from those that have an intrinsic personal value.

In a cross-border succession, the fate of the first type of assets is regulated by the *lex successionis*, being it either the law of the deceased's last habitual residence at the time of death, or the law of his/her nationality, should the deceased have chosen it. However, the transferability upon death of the digital assets created by contract can find a limit in the general terms and conditions agreed with the digital service provider if the terms provide for the termination of the contract upon the user's death. Conversely, when the terms and conditions do not regulate the matter, the principle of universality, coupled with the unitary approach, seems to confirm the transferability upon death of the digital assets.

When there is no succession in the deceased's account, and the digital assets have an intrinsic personal value, national law provisions regulate the heirs' rights – and the rights of everyone who has an interest in digital content – to access to those contents.

Lastly, an important planning role may be exercised by the deceased during his/her lifetime, since many digital service providers grant their users the rights to dispose to their digital content, either by prohibiting access to their data after their death or designating an heir contact.

As the digital society is at the dawn of its life, the law has not yet provided for all the solutions in order to manage smoothly the succession in the digital estate. Nevertheless, the field seems already well ploughed for further legislative actions and fruitful studies on the subject.

REFERENCES

BOOKS AND ARTICLES

1. Berlee, A., *Digital Inheritance in the Netherlands*, European Journal of Consumer and Market Law, Vol. 3, No. 6, 2017, pp. 256-260
2. Bonomi, A., *Successions internationales: conflits de lois et de juridictions*, Recueil des Cours, Vol. 350, 2011, pp. 71-418
3. de Miguel Asensio, P., *Conflict of Laws and the Internet*, Edward Elgar Publishing, Cheltenham-Northampton, 2020.

4. Fras, M., *Succession of digital goods. A comparative legal study*, Review of European and Comparative Law, Vol. 47, No. 4, 2021, pp. 67-81
5. Grahl-Madsen, A., *Conflict between the Principle of Unitary Succession and the System of Scission*, The International and Comparative Law Quarterly, Vol. 28, 1979, pp. 598-643
6. Harbinja E., *Digital Inheritance in the United Kingdom*, European Journal of Consumer and Market Law, Vol. 3, No. 6, 2017, pp. 253-256
7. Harbinja, E., *Digital Death, Digital Assets and Post-Mortem Privacy*, Edinburgh University Press, Edinburgh, 2023
8. Kuipers, J.-J., *Personality rights*, in: Basedow, J., Rühl, G., Ferrari, F., de Miguel Asensio, P. (eds.), Encyclopedia of Private International Law, Edward Elgar Publishing, Cheltenham-Northampton, 2017, pp. 1351-1359
9. Mackenrodt, M.-O., *Digital Inheritance in Germany*, European Journal of Consumer and Market Law, Vol. 4, No. 1, 2018, pp. 41-48
10. Maeschaelck, B., *Digital Inheritance in Belgium*, European Journal of Consumer and Market Law, Vol. 4, No. 1, 2018, pp. 37-41
11. Maniaci, A., d'Arminio Monforte, A., *"Eredità digitale" e accesso ai dati personali del defunto*, Diritto di Internet, No. 3, 2022, pp. 561-573.
12. Marino, M., *La successione digitale*, Osservatorio del diritto civile e commerciale, No. 1, 2018, pp. 167-204
13. Marino, M., *Mercato digitale e Sistema delle successioni* mortis causa, Edizioni Scientifiche Italiane, Napoli, 2022
14. Merchán Murillo, A., *La sucesión digital internacional y el Reglamento sucesorio europeo 650/2012*, Anuario español de derecho internacional privado, Vol. 21, 2021, pp. 327-357
15. Mosconi, F., *Oggetto e funzione*, in: Baratta, R. (a cura di), Diritto internazionale privato, Giuffrè, Milano, 2010, pp. 262-273
16. Palazzo, A., Sassi, A., *Trattato della successione e dei negozi successori*, Vol. 1, *Categorie e specie della successione*, Utet, Torino, 2012
17. Pazdan, M., Zachariasiewicz, M., *The EU succession regulation: achievements, ambiguities, and challenges for the future*, Journal of Private International Law, Vol. 17, No. 1, 2021, pp. 74-113
18. Queirolo, I., *Jurisdiction in succession matters: General rules and choice of court*, in: Bariatti, S., Viarengo, I., Villata, F.C. (eds.), EU Cross-Border Succession Law, Edward Elgar Publishing, Cheltenham-Northampton, 2022, pp. 219-243
19. Re, J., *Where Did They Live? Habitual Residence in the Succession Regulation*, Rivista di diritto internazionale privato e processuale, Vol. 54, No. 4, 2018, pp. 978-1009
20. Rühl, G., *Private international law, foundations*, in: Basedow, J., Rühl, G., Ferrari, F., de Miguel Asensio, P. (eds.), Encyclopedia of Private International Law, Edward Elgar Publishing, Cheltenham-Northampton, 2017, pp. 1380-1390
21. Spangaro, A., *La successione digitale: la permanenza* post mortem *di aspetti della personalità*, Giurisprudenza italiana, 2022, No. 6, pp. 1363-1370
22. Viarengo, I., *Planning Cross-Border Successions: the Professio Juris in the Succession Regulation*, Rivista di diritto internazionale privato e processuale, Vol. 56, No. 3, 2020, pp. 559-582

23. Villata, F.C., *Il regolamento (UE) 2023/114 relativo ai mercati delle cripto-attività: prime note con un occhio al diritto internazionale privato*, Rivista di diritto internazionale privato e processuale, Vol. 59, No. 3, 2023, forthcoming
24. Woodman, F.L., *Fiduciary Access to Digital Assets: A Review of the Uniform Law Conference of Canada's Proposed Uniform Act and Comparable American Model Legislation*, Canadian Journal of Law and Technology, Vol. 15, No. 2, 2012, pp. 193-227

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Joined Cases C509/09 and C161/10, eDate Advertising GmbH [2011] ECR I-10269

EU LAW

1. Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6
2. Regulation (EU) No 650/2012 of the European Parliament and of the Council on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L201/107
3. Regulation (EU) No 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1
4. Regulation (EU) 2016/679 of the European Parliament and of the Council 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), [2016] OJ L119/1
5. Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

France:

1. Law 7 October 2016 No 2016-1321 for a Digital Republic (pour une République numérique), Official Journal No 235/2016

Germany:

1. Bundesgerichtshof, 12 July 2018 III ZR 183/17, NJW, 2018, pp. 3178-3187

Italy:

1. Legislative Decree 30 June 2003 No 196, Personal Data Protection Code (Codice in materia di protezione dei dati personali), Official Journal No 174/2003
2. Tribunale di Milano, 10 February 2021
3. Tribunale di Bologna, 25 November 2021
4. Tribunale di Roma, 10 February 2022

WEBSITE REFERENCES

1. Apple, *iCloud condition No IV.D*, [https://www.apple.com/legal/internet-services/icloud/], Accessed 5 July 2023
2. UNIDROIT, *Draft UNIDROIT Principles on Digital Assets and Private Law*, [https://www.unidroit.org/wp-content/uploads/2023/01/Draft-Principles-and-Commentary-Public-Consultation.pdf], Accessed 5 July 2023
3. Uniform Law Commission, *Fiduciary Access to Digital Assets Act, Revised of 2015*, [https://www.uniformlaws.org/committees/community-home?communitykey=f7237fc4-74c2-4728-81c6-b39a91ecdf22], Accessed 5 July 2023

UDK 336.74-021.131:347.23
Original scientific paper

PROPERTY RIGHTS OVER CRYPTOCURRENCIES: A CONFLICT-OF-LAWS PERSPECTIVE*

Francesca C. Villata, PhD, Full Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
francesca.villata@unimi.it

Lenka Válková, PhD, Assistant Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
lenka.valkova@unimi.it

ABSTRACT

The paper tackles the conflicts of laws on property rights over cryptocurrencies, starting from characterization issues. Building upon the distinctive nature of cryptocurrencies as "pure" de facto assets, that do not give a claim against an issuer, and the relevance of control over said assets as a suitable alternative to the traditional possession, the paper supports the characterization in terms of "assets", over which property rights may, subject to the relevant lex causae, be constituted and enjoyed. By examining the available options for a conflict-of-law regime and considering the first legislative efforts conducted in this area of law both at the supranational and national level, the elective situs approach is identified as the most appropriate, possibly backed by some regulatory requirement, whilst different approaches are envisaged for the fall-back rule applicable to cryptocurrencies originated in, respectively, permissioned and permissionless DLT systems.

Keywords: *characterization, conflict of laws, cryptocurrencies, property rights, DLT systems*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. The present contribution is the result of common research and reflection of both authors and was prepared in their mutual collaboration. However, strictly regarding the process of drafting, it is specified for academic evaluation purposes that paragraphs 1 and 2.1 are to be attributed to Dr. Lenka Válková, whilst paragraphs 2.2, 3, and 4 are to be attributed to Prof. Francesca C. Villata.

1. INTRODUCTORY REMARKS ON CRYPTOCURRENCIES AND PIL ISSUES

According to Coinmarketcap,[1] as of February 2023 over 9000 different cryptocurrencies are traded globally and the worldwide crypto market cap amounts to USD 1,07 trillion.[2] Among them, Bitcoin is the best known[3] and most present on the market, with a market share of around 45% (even 65% in June 2020).[4] Moreover, Bitcoin was not only the prototype of all cryptocurrencies, revealed to the world by the legendary[5]

---

1 CoinMarketCap, *Today's Cyptocurrency Prices by Market Cap*, [https://coinmarketcap.com/], Accessed 28 February 2023.

2 Because of the recent collapse of important players in the crypto market, such as the FTX Exchange, and the consequent turbulences in the worldwide crypto market, the market cap has significantly decreased in size compared to November 2021, when it amounted to USD 2,47 trillion. *Cf* Conlon, T., Corbet, S., Hu, Y., *The Collapse of FTX: The End of Cryptocurrency's Age of Innocence*, SSRN, 2022, [https://ssrn.com/abstract=4283333 or http://dx.doi.org/10.2139/ssrn.4283333], Accessed 28 February 2023.

3 *Wright v McCormack* [2021] EWHC 2671 (QB), para. 5, whereby "[a] cryptocurrency is a digital asset designed to work as a medium of exchange, in which individual coin ownership records are stored in a ledger existing in a computerised database using cryptography to secure transactions, to control the creation of additional coins, and to verify the transfer of coin ownership. It does not exist in physical form (as paper money does) and is typically not issued by a central authority. Bitcoin is probably the best-known cryptocurrency." See also Karim, M.; Tomova, G., *Research Note: Cryptoasset consumer research 2021*, Financial Conduct Authority, 2021, [https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021], Accessed 28 February 2023.

4 European Parliament resolution with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets [2020] (2020/2034(INL)), P9_TA(2020)0265, Recital N.

5 "Satoshi Nakamoto" is the pseudonym used by the person, or persons, who developed Bitcoin. In that regard, a dispute was filed before English courts between Dr. Craig Wright, a national of Australia who has lived in the United Kingdom since December 2015 and is a computer scientist with a particular interest in cryptocurrencies, including Bitcoin, maintaining that he is Satoshi Nakamoto, and Roger Ver, a bitcoin investor and commentator on bitcoin and other cryptocurrencies, who was born in California, U.S., and moved to Japan, which he described in evidence as the global centre for cryptocurrencies, in 2005. In 2014 he renounced his US citizenship and became a citizen of St. Kitts & Nevis, although he continues to live in Japan. Mr. Ver does not accept that Dr. Wright is Satoshi Nakamoto. Dr. Wright claims that he was libeled by Mr. Ver in a YouTube video posted on the Bitcoin.com YouTube channel, a tweet containing the YouTube video, and a reply on Mr. Ver's Twitter Account posted from BkkShadow some 8 minutes after the tweet from Mr. Ver. These publications were alleged to be defamatory, in that Dr. Wright "had fraudulently claimed to be Satoshi Nakamoto, that is to say the person, or one of the group of people who developed Bitcoin." *Cf. Wright v Ver* [2020] EWCA Civ 672 (29 May 2020) declining English jurisdiction on the controversy, based on the argument "that England and Wales is not clearly the most appropriate place to bring this action for defamation." Furthermore, Dr. Wright also sued journalist Peter McCormack for defamation in 2019 over tweets or, a series of tweets, he had made in which he either directly, or by innuendo, called Wright a fraud for his claim that he was Bitcoin inventor Satoshi Nakamoto: *cf. Wright v McCormack* [2021] EWHC 2671 (QB).

Satoshi Nakamoto on 31 October 2008,[6] but it also represents the paradigm around which the legal discourse on distributed ledger technologies (DLTs) and crypto assets was, at least initially, developed.

Technological features of cryptocurrencies have been raising a number of challenges for lawyers and, namely, for private international lawyers, in that (i), cryptocurrencies are intangible, (ii) they exhibit a wide range of different financial features[7] that, to add further complexity, evolve in parallel with technological developments, (iii) the identity of cryptocurrency users – *i.e.*, everyone who is involved in the process of creation and transfer of cryptocurrencies[8] – is, at minimum, not easy to trace, since it is protected through pseudonyms or, even, full anonymity, (iv) they are set for more than one usage, *i.e.*, both as a payment instrument and a form of investment (albeit a very risky one!).[9] Even more relevant, (v) they have an intrinsically cross-border reach, since they are based on decentralized distributed ledgers, potentially spanned all over the world, with no connections to any particular state, allowing value to be transferred between users across borders at a very high speed, not conditional on the location of the transferor and the transferee. Finally, (vi) it is extremely difficult to impose legal restrictions on

---

6 Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin, 2009, [https://bitcoin.org/bitcoin.pdf], Accessed 28 February 2023.

7 *Cf.* European Central Bank (ECB), *Virtual currency schemes – a further analysis*, 2015, pp. 9 ff [https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf], Accessed 28 February 2023; and Houben R.; Snyers, A., *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, 2018, pp. 31 ss. [https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf], Accessed 28 February 2023, providing a synthetic description of the 10 cryptocurrencies with the highest market capitalization.

8 Yet, Article 14 of the Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, [2023] OJ L 150/1, requires that the crypto asset service provider of the originator ensures that transfers of crypto assets are accompanied by the name of the originator, the originator's account number, where such an account exists and is used to process the transaction, and the originator's address, official personal document number, customer identification number or date and place of birth. Moreover, the crypto asset service provider of the originator must ensure that transfers of crypto assets are accompanied by the name of the beneficiary and the beneficiary's account number, where such an account exists and is used to process the transaction. In that respect, it is worth mentioning that pursuant to Article 3 n 21 of the same Regulation "'originator' means a person that holds a crypto-asset account with a crypto-asset service provider, a distributed ledger address or a device allowing the storage of crypto-assets, and allows a transfer of crypto-assets from that account, distributed ledger address, or device, *or, where there is no such account, distributed ledger address, or device, a person that orders or initiates a transfer of crypto-assets*" (Italics added), whereby a "'distributed ledger address' means an alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where crypto-assets can be sent or received" (*cf* Article 3 note 18).

9 European Parliament resolution of 8 October 2020, *op. cit.*, note 4, Recital L.

their circulation, including territorial restrictions, not only because of the decentralized nature of said ledgers, but also because of their proclaimed inherent autonomy *vis-à-vis* the law. In fact, certain technical features of the systems on which the mere existence of cryptocurrencies depend, such as the automated functioning of those systems– based on smart contracts, as well as on consent mechanisms relying on cryptographic techniques, collective validation of the transactions, and continuous chains of blocks, unmodifiable without the consent of the majority of participants to the system (or good hacking skills…) –, make those systems not only tamper resistant, but also difficult to subjugate to any legal constraints.

Looking at cryptocurrencies from a legal perspective, according to the many definitions provided by various institutional players, in their attempt to grasp the distinctive features of cryptocurrencies that are relevant for the purpose of establishing a sound and effective legal framework, coherent with the policy objectives pursued by those institutions, the following elements have been commonly identified.

Firstly, the core of all definitions, including legislative ones,[10] lies in the notion of cryptocurrencies as digital representations of value,[11] originated in distributed led-

[10] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L41/73, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, [2018] OJ L156/43, and Directive (EU) 2019/2177 of the European Parliament and of the Council [2019] OJ L334/155, Art. 3 n 18 ("'virtual currencies'" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically") and Recital 10; *cf. e.g.*, the Italian implementing rule provided in decreto legislativo No. 231 of 21 November 2007, Gazz. Uff., No. 290 of 14 December 2007 - Suppl. Ord. No. 268, Art. 1 para. 2 *litt.* Qq, as amended by Art. 1 para. 1 *litt* h of decreto legislativo No. 125 of 4 October 2019, Gazz. Uff., No. 252 of 26 October 2019: "valuta virtuale: la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente." See also Uniform Law Commission, Uniform Regulation of Virtual-Currency Businesses Act (URVCBA), Sec. 102 n 23: "'Virtual currency:' (A) means a digital representation of value that: (i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender, whether or not denominated in legal tender;" Lehmann, M., *National Blockchain Laws as a Threat to Capital Markets Integration*, Uniform Law Review, Vol. 26, No. 1, 2021, pp. 162 ff.

[11] He, D. *et al.*, *Virtual Currencies and Beyond: Initial Considerations (IMF Staff Discussion Note)*, International Monetary Fund, 2016, p. 7, [https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf], Accessed 28 February 2023; European Banking Authority (EBA), *EBA Opinion on 'Virtual Currencies'*, 2014, p. 20, para. 11, [https://www.eba.europa.eu/sites/default/documents/files/docu-

gers via a process called "mining,"[12] making use of those ledgers to allow remote peer-to-peer exchanges of that value[13] and relying on cryptographic techniques to achieve consensus on the validation of the transfer.[14] Cryptocurrencies are not *per se* legal tender (unless any state or other monetary authority establish that they are),[15]

---

ments/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1] ("EBA Opinion"), Accessed 28 February 2023: "This part of the definition refers to the fact that the value is essentially represented in digital form. This does not exclude the possibility that it may also be physically represented, such as through paper printouts or an engraved metal object. The term 'digital representation of value' is close to the monetary concept of a 'unit of account' but includes the option to consider VCs as private money or a commodity. It also avoids making reference to a standard numerical unit of account for the measurement of value and costs of goods, services, assets and liabilities, which might (according to some views), imply that it needs to be stable over time."

12 Houben, Snyers, *op. cit.*, note 7, p. 32.

13 Bank for International Settlements, Committee on Payments and Market Infrastructures, *Digital Currencies*, 2015, p. 5, [https://www.bis.org/cpmi/publ/d137.htm], Accessed 28 February 2023; Kleiner, C., *Cryptocurrencies as Transnational Currencies?*, in: Benicke C; Huber S. (eds.), National, International, Transnational: Harmonischer Dreiklang im Recht. Festschrift für Herbert Kronke zum 70. Geburtstag, Bielefeld, 2020, pp. 979 ff.

14 World Bank Group (Harish Natarajan, Solvej Krause, and Harish Gradstein), *Distributed Ledger Technology (DLT) and blockchain (FinTech Note No. 1)*, World Bank, 2017, IV, [http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf], Accessed 28 February 2023; U.S. President Executive Order on Ensuring Responsible Development of Digital Assets of 9 March 2022, Sec. 9(c), [https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/], Accessed 28 February 2023.

15 On 7 September 2021, El Salvador became the first country to adopt Bitcoin as a legal tender. *Cf.* Asamblea Legislativa, El Salvador, the first country in the world to recognize Bitcoin as legal tender, Asamblea Legislativa, 2021, [https://www.asamblea.gob.sv/node/11282], Accessed 28 February 2023. While the law maintains the U.S. dollar as the national unit of account, it mandates the acceptance of Bitcoin by agents unless technical impediments exist. A new digital means of payments, *i.e.*, the e-wallet Chivo operating in both U.S. dollars and bitcoin, has been introduced and heavily supported by the government to promote financial inclusion (each qualifying citizen who downloaded the application received an endowment of USD 30). This led to protests and resulted in skepticism from economists and others. As a result, El Salvador President Nayib Bukele tweeted in August that businesses did not have to accept bitcoin. The law also guarantees the automatic conversion from bitcoin to U.S. dollars through a trust fund funded with USD 150 million from the budget, and in practice the conversion is done in Chivo. Later on, in International Monetary Fund, *Staff Concluding Statement of the 2021 Article IV Mission*, 2021, [https://www.imf.org/en/News/Articles/2021/11/22/mcs-el-salvador-staff-concluding-statement-of-the-2021-article-iv-mission], Accessed 28 February 2023, the IMF concluded that "[g]iven Bitcoin's high price volatility, its use as a legal tender entails significant risks to consumer protection, financial integrity, and financial stability. Its use also gives rise to fiscal contingent liabilities. Because of those risks, Bitcoin should not be used as a legal tender. Staff recommends narrowing the scope of the Bitcoin law and urges strengthening the regulation and supervision of the new payment ecosystem. Like for other e-wallets, Chivo should be required to fully safeguard customers' funds, both in U.S. dollars and Bitcoin, by segregating and ring-fencing reserve assets. Stronger regulation and oversight of the new payment ecosystem should be immediately implemented for consumer protection, anti-money laundering and counter financing of terrorism (AML/CFT), and risk management.

neither are they issued by a central bank or public authority,[16] nor necessarily attached to a fiat currency,[17] but they may well be converted into fiat currencies and vice versa,[18] their economic value being determined by supply and demand.[19] Accordingly, despite their volatility,[20] cryptocurrencies are "designed to work as a medium of exchange"[21] and, actually, as acknowledged by certain pieces of legislation, are "accepted by natural or legal persons as a means of exchange and… can be transferred, stored and traded electronically."[22] Moreover, in fact, cryptocurrencies may represent an investment vehicle, though a rather risky one, whereby their status as a store of value is largely dependent on their success as medium of exchange, hence, the rise of stablecoins, which are established with the purpose of eliminating the volatility of traditional cryptocurrencies by consistently holding a stable value. In most cases, one unit of a stablecoin is "pegged" at the value of the US dollar or the Japanese yen (fiat-backed).

The aforementioned characteristics of cryptocurrencies and, in particular, their intrinsic cross-border reach prompt the question of their Private International Law regime and, namely, (i) the need to identify, among the existing PIL rules, those which are applicable to property rights over cryptocurrencies and to investigate

---

Banking regulation should incorporate prudential safeguards such as conservative capital and liquidity requirements related to Bitcoin exposure. Measures to limit fiscal contingent liabilities, such as winding down the trust fund or withdrawing public subsidies to Chivo, should also be promptly considered."

16 European Securities and Markets Authority (ESMA), European Banking Authority (EBA), and European Insurance and Occupational Pensions Authority (EIOPA), *ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*, 2018, p. 1, [https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf], Accessed 28 February 2023.

17 EBA Opinion, *op. cit.*, note 11), 7. According to the European Central Bank, *Virtual Currency Schemes*, 2012, p. 14, [https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf], Accessed 28 February 2023, cryptocurrencies fall under the notion of "virtual currency schemes with bidirectional flow," in that users can buy and sell virtual money according to the exchange rates with their currency so that the virtual currency is "similar to any other convertible currency with regard to the interoperability with the real world;" *cf.* Houben, Snyers, *op. cit.*, note 7, pp. 21-22; Bocchini, R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, Il diritto dell'informazione e dell'informatica, Vol. 33, No. 1, 2017, p. 39.

18 Houben, Snyers, *op. cit.*, note 7, p. 23.

19 Bank for International Settlements, *op. cit.*, note 13, p. 4; Financial Markets Law Committee, *Issues of Legal Uncertainty Arising in the Context of Virtual Currencies*, 2016, p. 4, [http://fmlc.org/wp-content/uploads/2018/03/virtual_currencies_paper_-_edited_january_2017.pdf], Accessed 28 February 2023.

20 See, *e.g.*, European Central Bank, *op. cit.*, note 7, p. 16.

21 U.S. President Executive Order*, op. cit.,* note 14; *Wright*, *op. cit.*, note 3.

22 Directive (EU) 2015/849, n 10, Art. 3 n 18; European Parliament resolution of on virtual currencies, [2016] OJ/C 76; decreto legislativo No. 90 of 25 May 2017, Art. 1 para. 2 *litt* qq, Gazz. Uff., No. 140 of 19 June 2017 - Suppl. Ord. No. 28.

whether those rules are suitable for framing them, either in terms of legal characterisation or of connecting factors and other techniques to establish the applicable law. If and to the extent that the answer to the first question is negative, this paper will then explore (ii) if cryptocurrencies deserve, also in light of their growing economic relevance, or require, because of their potential systemic relevance, differentiated PIL rules, not only in comparison to traditional assets, but also in relation to other crypto-assets, depending upon their intrinsic technical features and/or their use case, and (iii) whether territorial connecting factors are still relevant for or can apply at all to that context or, instead, whether different (combinations) of PIL techniques could be more fit for purpose.

Notwithstanding the aforementioned technical difficulties and irrespective of both the expectations of the participants to a blockchain system and certain scholarly assertions,[23] blockchain transactions cannot, actually, eschew the law, nor should parties to those transactions have an interest in keeping completely away from the law: at least, this is the case insofar as they wish to be able to rely on the enforcement mechanisms that only state authority has the power to operate, should any player involved in said transactions behave unfairly or be unable to perform its functions in the relevant transaction scheme.[24] Therefore, the present paper aims to provide some (tentative) answers to the three questions set out above, starting from the basic issue of characterisation.

2. CHARACTERISATION OF CRYPTOCURRENCIES

From a legal perspective, the classification of cryptocurrencies is (very) far from being definite, let alone uniform, under domestic laws and, as it is often the case, it may well vary, depending upon the origin (national or supranational), the scope, and the objectives of the relevant piece of legislation.

2.1. "Cryptocurrencies" under National Substantive Laws

English case-law and scholars have progressively converged on the idea of a cryptocurrency as a "particularly odd type of incorporeal"[25] or "intangible personal property," insofar as, unlike *choses* in action, they do not themselves constitute a

[23] Wright A.; De Filippi, P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN, 2015, p. 48 [https://papers.ssrn.com/abstract=2580664], Accessed 28 February 2023.

[24] See EBA Opinion, *op. cit.*, note 14, p. 23 ff for an assessment of risks that can arise from virtual currencies

[25] Carr, D., *Cryptocurrencies as Property in Civilian and Mixed Legal Systems*, in: Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, p. 180 f para. 7.07.

right which has a concomitant obligation in another.[26] Namely, cryptocurrencies are deemed to possess the characteristics of property, as summarised in *National Bank v Ainsworth*,[27] which entails that they are "definable, identifiable by third parties, capable in [their] nature of assumption by third parties and have some degree of permanence and stability" according to the assessment conducted by the UK Jurisdiction Taskforce[28] endorsed by subsequent jurisprudence.[29] Following a call for evidence, on 24 November 2021 the Law Commission published an

---

[26] Fox, D., *Cryptocurrencies in the Common Law of Property*, in: Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, pp. 150 ff.

[27] *National Provincial Bank v Ainsworth* [1965] UKHL 1, 19.

[28] Financial Markets Law Committee, note 19, pp. 5, 23; UK Jurisdiction Taskforce, *Legal statement on crypto-assets and smart contracts*, Tech Nation, 2019, pp. 49-57, [https://technation.io/about-us/law-tech-panel], Accessed 28 February 2023. The UK Jurisdiction Taskforce is one of the six taskforces of the LawTech Delivery Panel within The Law Society of England and Wales. According to the website of The Law Society, [https://www.lawsociety.org.uk/campaigns/lawtech/guides/lawtech-delivery-panel], the LawTech Delivery Panel is "a team of industry experts and leading figures from government and the judiciary, has been formed to help the UK legal sector grow and fulfil its potential. By identifying both barriers to and catalysts for growth, the panel will provide direction to the legal sector and help foster an environment in which new technology can thrive." The position taken by the UK Jurisdiction Taskforce had been anticipated, albeit concisely, in a couple of judgments: *Vorotyntseva v MONEY-4 Ltd (t/a nebeus.com) & Ors* [2018] EWHC 2596 (Ch), 13; *Liam David Robertson v Persons Unknown* (unreported), quoted *in AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm), 13.

[29] *Ion Science & Duncan Johns v Persons Unknown* (unreported) (21 December 2020), 13, as summarized by Sleave, L., *Cryptocurrency Fraud - The High Court Considers The Position Of 'Crypto-assets'*, Mondaq Business Briefing, 2021, [https://link.gale.com/apps/doc/A663644295/ITOF?u=milano&sid=bookmark-ITOF&xid=03ffe69d], Accessed 28 February 2023. The case is said to have arisen from proceedings brought by Ion Science Limited (ISL) and its sole director Duncan Johns, who claimed to be victims of a cryptocurrency initial coin offering, or ICO, fraud. Mr. Johns claimed he was persuaded by an individual, Ms. Black, said to be connected to a Swiss entity called Neo Capital, to transfer funds which were converted into Bitcoin by Ms. Black, granting Ms. Black remote access to his computer to manage this. Mr. Johns also made further transfers to an escrow account, claiming Ms. Black informed him these payments were needed to release commission payments from one of the investments, the Oileum ICO. Allegedly, the applicants subsequently discovered that Neo Capital was not a real company and that the Swiss regulator had issued a warning that it may be providing unauthorised services. Neither Mr. Johns nor ISL received any profits supposedly made in relation to the Oileum ICO or received back any of the funds invested. The court heard evidence from an expert in cryptocurrency fraud who concluded that (i) a substantial part of the bitcoins transferred or their traceable proceeds were held by the Binance and Kraken cryptocurrency exchanges; and (ii) both exchanges held information about the customers to whom those accounts belong. Alleging the sums invested had been misappropriated, the applicants applied for a proprietary injunction, a worldwide freezing order, and an ancillary disclosure order against persons unknown, the individuals or companies describing themselves as being or connected to Neo Capital. In addition, the applicants sought a disclosure order against Binance Holdings Limited, a Cayman company believed to be the parent of the group of companies that operates the Binance Cryptocurrency Exchange and Payments Ventures, a US entity believed to be the parent of the group of companies that operates the Kraken Cryptocurrency Exchange. The applicants further asked for permission to serve the proceedings out of the jurisdiction and by alternative means. Drawing (also) on analysis of the position in the UK Jurisdiction Taskforce, note 28, the court found there was at least a serious issue to be tried that Bitcoin was property under the common law

"Interim Update" concerning the "Digital Asset Project," [30] whereby, while "acknowledging that 'digital asset is an extremely broad term that requires further subdivision,'" it "recognise[d] that certain digital assets could fall within a new 'third category' of personal property."[31] Subsequently, on 28 July 2022, the Law Commission, in its "Digital assets: Consultation paper",[32] has conceptualized the proposed new category named "data objects", based on the following criteria: (i) the thing in question must be composed of data represented in an electronic medium, including in the form of computer code, electronic, digital or analogue signals;[33] (ii) it must exist independently of persons and exist independently of the legal system;[34] (iii) it must be rivalrous;[35] whilst divestibility – that is an inherent characteristic of a rivalrous tangible object –, is rather presented as a likely consequence of the fact that a particular object meet the second and the third criterion, given the possibility to create an independently existing, rivalrous digital asset that cannot be transferred as a matter of design (other than by destroying it).[36] Finally, although the Law Commission, in its "Digital assets: Final report",[37] following negative feedbacks received on the aforesaid three criteria, concluded that it is "not necessary or appropriate" for legislation to define the boundaries of such a third category,[38] it has acknowledged digital assets "as things to which personal property rights can relate".[39]

The classification as property has also been upheld by Singapore[40] and Russia,[41] as well as certain Italian judgments.[42]

---

definition. See also *AA*,, *op. cit.*, note 28, 59; *Fetch.AI Lrd & Anor v Persons Unknown Category A & Ors* [2021] EWHC 2254 (Comm), 9.

30 Law Commission, *Digital Assets Interim Update*, 2021, 1.14-1.17 [https://www.lawcom.gov.uk/project/digital-assets/], Accessed 28 February 2023.

31 The view is confirmed in *Osbourne v Persons Unknown Category A & Ors* [2023] EWHC 39 (KB) (13 January 2023), 18.

32 Law Commission, *"Digital assets: Consultation paper"*, No 256 of 28 June 2022, [https://www.lawcom.gov.uk/document/digital-assets-consultation-paper/], Accessed 28 February 2023.

33 *Ibid.*, para. 5.14 ff.

34 *Ibid.*, para. 5.22 ff.

35 *Ibid.*, para. 5.48 ff.

36 *Ibid.*, para. 5.85 ff.

37 Law Commission, *"Digital assets: Final report"*, No 412 of 23 June 2023, [https://www.lawcom.gov.uk/document/digital-assets-final-report-2/], Accessed 20 July 2023.

38 *Ibid.*, para. 3.8.

39 *Ibid.*, para. 3.9 ff.

40 *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, 142, quoting *National Provincial Bank*, *op. cit.*, note 27.

41 Haentjens, M.; De Graaf, T.; Kokorin, I., *The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them*, Singapore Journal of Legal Studies, No. 2, 2020, p. 551.

42 Tribunale di Firenze, 19 December 2018, No. 6, I Contratti, 2019, pp. 661-669, note Fauceglia, D., *Il deposito e la restituzione delle criptovalute*, I Contratti, No. 6, 2019, pp. 669-680; Tribunale di Firenze

On the other hand, in the statement above, the UK Jurisdiction Taskforce has included crypto-assets in general among "conventional financial assets."[43] Along the same lines, the German Federal Financial Supervisory Authority ("BaFin") issued a communication, according to which "[i]n accordance with BaFin's legally binding decision on units of account within the meaning of section 1(11) sentence 1 of the *KWG* [Banking Act – *Kreditwesengesetz*], bitcoins are financial instruments" and, namely, "units of account… comparable to foreign exchange with the difference that they do not refer to a legal tender."[44] Following a successful challenge in court, the German legislator has introduced a new provision into the *KWG* defining crypto assets (*Kryptowerte*) as financial instruments.[45] However, pursuant to § 2 para. 3 of the *EWpG* [Electronic Securities Act – *Gesetz über elektronische Wertpapiere*] of 3 June 2021, an electronic security is deemed to be a moveable ("*Sache*") within the meaning of Section 90 of the German Civil Code.[46]

Turning to the other side of the Atlantic Ocean, in July 2018 the Uniform Law Commission adopted the "Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act" ("USCL for URVCBA") and recommended its enactment in all the United States.[47] According to Section

(Sez. fall.), 21 January 2019, No. 18, Giurisprudenza italiana, 2020, pp. 2657-2659; note Fauceglia, D., *Scambio e deposito di criptovalute: la responsabilità del gestore della piattaforma*, Giurisprudenza italiana, No. 18, 2020, pp. 2659-2666.

43 UK Jurisdiction Taskforce, *op. cit.*, note 28, p. 52.

44 German Federal Financial Supervisory Authority ("BaFin"), *Virtual Currency (VC)*, 2017, [https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html], Accessed 28 February 2023. Along the same line of reasoning see Cassazione Penale (Sez. II), 17 September 2020, No. 26807, Giurisprudenza italiana, 2021, pp. 2224-2225, note Vadalà, R. M., *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, Giurisprudenza italiana, 2021, pp. 2225-2231.

45 See section 1(11) no. 10 of the *KWG*. In section 1(11) sentence 4 of the *KWG*, crypto assets are defined as a digital representation of value which has neither been issued nor guaranteed by a central bank or public body; it does not have the legal status of currency or money but, on the basis of an agreement or actual practice, is accepted by natural or legal persons as a means of exchange or payment or serves investment purposes; it can be transferred, stored, and traded by electronic means. See German Federal Financial Supervisory Authority ("BaFin"), *Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG)*, BaFin, 2020, [https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html?nn=9451720#O4], Accessed 28 February 2023.

46 Gesetz über elektronische Wertpapiere (eWpG) vom 3. Juni 2021 (*BGBl.* I S. 1423), § 2 para. 3: "Ein elektronisches Wertpapier gilt als Sache im Sinne des § 90 des Bürgerlichen Gesetzbuchs".

47 The Final Text can be retrieved at the Uniform Law Commission website, namely [https://www.uniformlaws.org/viewdocument/final-act-154?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778&tab=librarydocuments], Accessed 28 February 2023. See Zachary Hubbell, *The Uniform Regulation of Virtual-Currency Business Act: Advancing State Regulatory Interests in a Truly Cashless Economy*, Jurimetrics, Vol. 59, 2019, p. 313.

4, by virtue of agreement between parties to virtual currency transactions, the virtual currency may be "treated as a financial asset credited or held for credit to the securities account of the user," thereby collocating said transactions into the realm of Article 8 of the Uniform Commercial Code (UCC). As it has been rightly pointed out, however, the notion of securities entitlement embodied in Article 8 UCC – whereby holders of securities are granted with a claim for securities against the relevant intermediary – seems "incongruous" with the pattern of traceability that is commonly reconnected with crypto assets because of the DLTs supporting the creation and "transfer" of said assets. Therefore, Section 502(a) URVCBA requires that "A licensee or registrant that has control of virtual currency for one or more persons (…) maintain in its control an amount of each type of virtual currency sufficient to satisfy the aggregate entitlements of the persons to the type of virtual currency." [48] Anyway, according to Section 7 USCL for URVCBA "Treatment of virtual currency as a financial asset credited to a securities account under this [act] and Article 8 does not determine the characterization or treatment of the virtual currency under any other statute or rule."

In fact, on 10 June 2021, the Securities and Exchange Commission (SEC)'s Office of Investor Education and Advocacy (OIEA) and the Commodity Futures Trading Commission (CFTC)'s Office of Customer Education and Outreach (OCEO) published an "Investor Bulletin," whereby, while urging "investors considering a fund with exposure to the Bitcoin futures market to weigh carefully the potential risks and benefits of the investment," in light of "the volatility of Bitcoin and the Bitcoin futures market, as well as the lack of regulation and potential for fraud or manipulation in the underlying Bitcoin market," expressed the view that "in the United States, Bitcoin is a commodity, and commodity futures trading is required

[48] However, whilst Rhode Island enacted the above mentioned provisions of the USCL for URVCBA – namely under R.I. Gen. Laws § 6-56-1-6-56-11 (Current through Chapter 429 (all legislation) of the 2021 Session, including all corrections and changes made by the Director of Law Revision), [https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DF-62M1-DYB7-W0YY-00000-00&context=1516831], Accessed 28 February 2023; Wyoming has followed a different approach, whereby a digital asset, even if treated as a financial asset for the purpose of art 8 UCC, shall remain intangible personal property. Moreover, according to said provision, "[v]irtual currency is intangible personal property and shall be considered money;" see § 34-29-102. Classification of digital assets as property; applicability to Uniform Commercial Code; application of other law., Wyo. Stat. § 34-29-102 (Current through 2021 General Session and Special Session of the Wyoming Legislature. Subject to revisions by LSO), [https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DC-SNC3-CH1B-T54F-00000-00&context=1516831], Accessed 28 February 2023. See Lehmann, *op. cit.*, note 10, p. 164 f.; Crockett, M., *Wyoming's DIY Project Gets Western with the UCC*, Wyoming Law Review, Vol. 20, No. 1, 2020, p. 105; Hughes, S. J., *Property, Agency, and the Blockchain: New Technology and Longstanding Legal Paradigms*, Wayne Law Review, Vol. 65, 2019, p. 57. Wyo. Stat. § 34-29-102.

to take place on futures exchanges regulated and supervised by the CFTC."[49] Although the "Investor Bulletin" only represents the views of the staff of the SEC's Office of Investor Education and Advocacy and CFTC's Office of Customer Education and Outreach and it is not a rule, regulation, or statement of the SEC or the CFTC, on 28 September 2021 the latter authority issued an order, filing and settling of charges against Payward Ventures, Inc. d/b/a Kraken, one of the cryptocurrency industry's largest market participants, for offering margined retail commodity transactions in cryptocurrency -– including Bitcoin – and failing to register as a futures commission merchant (FCM).[50] Moreover, according to the definition adopted in the U.S. President Executive Order on Ensuring Responsible Development of Digital Assets of 9 March 2022, Sec. 9(c) "cryptocurrencies" refers to "a digital asset (…) for which *generation or ownership* records are supported through a distributed ledger technology".[51] Finally, on 21 February 2023 the Uniform Law Commission and the American Law Institute made available the Uniform Commercial Code Amendments (2022), which provide a new UCC Article 12 that governs the transfer of property rights in certain intangible digital assets ("controllable electronic records") that have been or may be created and may involve the use of new technologies, including (non-fiat) virtual currency.[52]

A different approach has been followed under the Swiss Act to Adapt Federal Law to Developments in Distributed Ledger Technology ("DLT Act"), some parts of which entered into force on 1 February 2021.[53] That piece of legislation, actually,

---

[49] The joint statement is contained in US Securities and Exchange Commission, *Funds Trading in Bitcoin Futures – Investor Bulletin*, 2021, [https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/funds], Accessed 28 February 2023.

[50] The CFTC alleged that each of the defendants was acting as an unregistered FCM. Under Section 1a(28)(a) of the Commodity Exchange Act, 7 U.S.C. § 1(a)(28)(A), an FCM is any "individual, association, partnership, or trust that is engaged in soliciting or accepting orders for the purchase or sale of a commodity for future delivery; a security futures product; a swap… any commodity option authorized under section 6c of this title; or any leverage transaction authorized under section 23 of this title." To be considered an FCM, that entity must also "accept money, securities, or property (or extends credit in lieu thereof) to margin, guarantee, or secure any trades or contracts that result or may result therefrom." See 7 U.S.C. § 1(a)(28)(A)(II). 7 U.S.C. § 6d(1) requires FCMs to be registered with the CFTC. See Evans, J. B.; Scheibe, A. C., *A Flurry of CFTC Actions Shock the Cryptocurrency Industry*, McDermott, 2021, [https://www.mwe.com/it/insights/a-flurry-of-cftc-actions-shock-the-cryptocurrency-industry/], Accessed 28 February 2023.

[51] U.S. President Executive Order, *op. cit.*, note 14, emphasis added.

[52] Uniform Commercial Code Amendments, 2022, [https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac#:~:text=The%202022%20amendments%20to%20the,intelligence%2C%20and%20other%20technological%20developments], Accessed 28 February 2023.

[53] Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 25. September 2020, RO 2021 33. The Act to Adapt Federal Law to Developments in Distributed Ledger Technology (DLT Act) has been complemented with an Order (Verordnung zur

acknowledges the distinction between tokens in the form of cryptocurrencies, that are classified as intangible assets under civil law, for which that law does not provide any specific requirements nor obstacles to their transfer, and a new category of ledger-based securities (*Registerwertrecht*) that is introduced in the Code of Obligations (*Obligationenrecht*, OR, Art. 622 para 1; Art. 973d).[54] The wording of the provision is technology-neutral and does not mention the term DLT, but describes its characteristics instead. A ledger-based security is defined as a right that, according to an agreement of the parties, is registered in a ledger-based security register and can be asserted and transferred only via this register (Art. 973d para 1 OR). The ledger-based security register must fulfil the following requirements: it gives creditors, but not the debtor, power of disposal over their assets by means of a technical process. Its integrity is protected through appropriate technical and organizational measures to prevent unauthorized modifications, such as joint management by several participants that are independent of each other. The content of the rights, the functioning of the register, and the register agreement are recorded in the register or in the accompanying data. Creditors may access information and register entries that concern them, and may test the integrity of the register entry that concerns them without the help of third parties (Art 973d para 2 OR). Debtors of ledger-based securities are obligated and allowed to render performance only to a creditor whose name is registered in the ledger-based security register (Art. 973e para 1 OR). A *bona fide* purchaser may rely on the content of the register (protection of good faith) (Art 973e para 3 OR). The transfer of the ledger-based security is subject to the terms of the registry agreement (Art. 973f para 1 OR). According to Article 973c ff OR, ledger-based securities are, thus, equated, in many respects, to negotiable instruments and the Federal Act on Private International Law (PILA) of 18 December 1987 has been amended accordingly (see especially Article 145a PILA).[55] Moreover, the DLT Act has been complemented with an Order to introduce further amendments into Swiss financial markets law.[56]

2.2. Towards a Common Understanding of Cryptocurrencies

The aforesaid attempts to frame cryptocurrencies into substantive law clearly show, firstly, that they are not treated as the cryptographic strings of characters that they in

Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 18. Juni 2021, RO 2021 400) to introduce further amendments into Swiss financial markets law.

54 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220 (Swiss Civil Code of Obligations).

55 Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987, SR 291.

56 Ordinanza del Consiglio federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito del 18 giugno 2021, RO 2021 400.

fact are, *i.e.* data or information, but rather for the notional status that they have,[57] which is based on an implicit agreement or, rather, expectations, between participants to the systems where cryptocurrencies are created and transferred, that those strings actually represent a value, resulting from supply and demand balancing, and that "the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system and the power to deal with those units."[58] Second, the classification of cryptocurrencies varies depending on the diverse use cases, *i.e.* store of value, tools for investment or means of payment. Third, the notional value of cryptocurrencies, their status as creatures of the law (albeit the law here is, at least at the outset, a code), and the fact that, because of the notional embodiment of the value in cryptographic strings, they represent a safe vehicle to transfer value from one person to another,[59] on one hand, might place cryptocurrencies in the realm of negotiable instruments (or even of money) and, on the other hand, those very same features, are a driver for their use as investment vehicles.

2.2.1. Cryptocurrencies as "Purely de facto Assets"

However, along the many discussions concerning the intrinsic nature of cryptocurrencies, there is a common understanding that cryptocurrencies, and especially those modelled on bitcoins, neither represent nor give a claim against an issuer,[60] hence the classification as "purely *de facto* assets" acknowledged, for instance, in the Swiss Federal Council message accompanying the proposal for the DLT Act.[61] This seems to be the key distinctive feature of "pure" cryptocurrencies from other crypto-assets, including stablecoins,[62] which may also be used and accepted as payment instruments.

---

57 Fox, *op. cit.*, note 26, para. 6.18.

58 Dickinson, A., *Cryptocurrencies and the Conflict of Laws*, in: Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, para. 5.107.

59 Fox, *op. cit.*, note 26, para. 6.18.

60 EBA Opinion, *op. cit.*, note 11, para. 30; Financial Conduct Authority (FCA), *Guidance on Crypto-assets (Consultation Paper CP19/3)*, 2019, paras. 3.35, 3.60, [https://www.fca.org.uk/publication/consultation/cp19-03.pdf], Accessed 28 February 2023; Swiss Federal Council, *Legal framework for distributed ledger technology and blockchain in Switzerland. An overview with a focus on the financial sector*, Report, 2018, p. 46, para. 5.1.2.1, [https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf], Accessed 28 February 2023; Barsan, I. M., *Legal Challenges of Initial Coin Offerings (ICO)*, Revue Trimestrielle de Droit Financier (RTDF), No. 3, 2017, p. 58; Fox, *op. cit.*, note 26, para. 6.30; Carr, *op. cit.*, note 25, p. 180 f, para. 7.07.

61 See Messaggio concernente la legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito del 27 novembre 2019, FF 2020 223, 232.

62 ECB Crypto-Assets Task Force, *Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area*, Occasional Paper Series No. 247,

Notably, the Proposal for an EU Regulation on Markets in Crypto-assets,[63] as resulting from the latest steps of the legislative procedure, seemed to acknowledge that distinction, insofar as it provided for a differentiated treatment between e-money token, the users of which should have been granted with a claim on the issuer of such tokens, *i.e.* the right to redeem their tokens at any moment and at par value against the currency referencing those tokens, and "other crypto-asset referencing one official currency of a country" that "do not provide a claim at par with the currency they are referencing or limit the redemption period."[64] Namely, the Proposal provided for different regimes, respectively, for "asset referenced tokens" (Title III of the Proposal),[65] "electronic money tokens" (Title IV) and "crypto-assets, other than asset referenced tokens or electronic money tokens" (Title II), including, but not limited, to utility tokens.[66] Moreover, for the purpose of the Proposal, the definition of "crypto asset" referred to "a digital representation *of a value* or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology,"[67] whereby "[r]epresentation of value includes external, non-intrinsic value attributed to a crypto-asset by parties concerned or market participants, meaning the value can be subjective and can be attributed only by the interest of someone purchasing the crypto-asset."[68]

2020, p. 8, [https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf], Accessed 28 February 2023.

63 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [2020] COM/2020/593 final, Art. 44 (hereinafter "MiCA Proposal").

64 See the final compromise text of the *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937* accompanying as an Annex the Council of the European Union, Letter to the Chair of the European Parliament Committee on Economic and Monetary Affairs, doc. 13198/22 of 5 October 2022*,* Recital 10 (hereinafter, 'Council final compromise text'), and European Parliament Economic and Social Committee, *Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937* (A9-0052/2022 pf 17 March 2022), Recital 10 (hereinafter, 'ESC Report'). Accordingly, the EBA had previously pointed out that "the difference between electronic money and a virtual currency is that the latter is not necessarily attached to a FC [i.e., a fiat currency], *i.e.* it does not have a fixed value in a FC and, furthermore, is not necessarily fixed to be redeemed at par value by an issuer." EBA Opinion*, op. cit.,* note 11, para. 31. The view is upheld also by the Financial Conduct Authority, note 57, p. 31 para. 3.61.

65 According to Zetzsche, D. A. *et al*, *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*, EBI Working Paper Series No. 2020/77, SSRN, 2020, p. 12 [http://dx.doi.org/10.2139/ssrn.3725395], Accessed 28 February 2023, the proposed global stablecoin Libra would fall under this category. See *infra* (note 73).

66 Council final compromise text, *op. cit.*, note 64, Recital 9, and ESC Report, *op. cit.*, note 61, Recital 9.

67 Council final compromise text, *op. cit.*, note 64, Art. 3 para. 1(2) (emphasis added). The Economic and Social Committee of the European Parliament has specified the notion of "digital representation" by adding the requirement that it "is in the form of a coin or a token or any other digital medium": see ESC Report, *op. cit.*, note 61, Art. 3 para. 1(2).

68 Council final compromise text, *op. cit.*, note 64, Recital 2.

Therefore, despite the claim that "any definition of 'e-money tokens' should be as wide as possible to capture all the types of crypto-assets referencing one single official currency of a country" and that "strict conditions on the issuance of e-money tokens should be laid down, including the obligation for such e-money tokens to be issued either by a credit institution as defined in Regulation (EU) No 575/2013 of the European Parliament and of the Council, or by an electronic money institution authorised under Directive 2009/110/EC,"[69] "pure" cryptocurrencies seemed to fall under the residual category of "other crypto assets."[70] The same Proposal envisaged a more general distinction between crypto assets that may qualify as "financial instruments as defined in Article 4(1), point (15), of Directive 2014/65/EU" (*i.e.*, MiFID II Directive)[71] (or as deposits, funds, securitisation positions, insurance or pension products according to the respective relevant EU provisions,[72] which, incidentally, should be neutral as regards the use of technology),[73] and those which are not covered by those regimes and are, accordingly, included in the scope of the Proposal, with the additional aforesaid sub-distinction. With regard to pure payment-type crypto assets, however, the European Securities and Markets Authority (ESMA), in its "Advice" concerning "Initial Coin Offerings and Crypto-Assets" of 9 January 2019 held as "unlikely" that they qualify as financial instruments.[74]

The general notion of "crypto-asset", as well as the aforementioned tripartition, have been upheld in the final text of the MiCA Regulation.[75] It might worth noticing, however and with specific regard to bitcoins (and the alikes), that, despite the general statement that the new Regulation "covers the rights and obligations of issuers of crypto-assets, offerors, persons seeking admission to trading of crypto-

---

69 *Ibid.*, Recital 10.

70 Also, Zetzsche *et al*, *op. cit.*, note 62, p. 25, seem to concur with this view.

71 See Council final compromise text, *op. cit.*, note 64, Art. 2 para. 3 *litt.* a and Recital 3. The Economic and Social Committee, "because of the specific features linked to their innovative and technological aspects", has recalled the need "to identify clearly the requirements for classifying a crypto-asset as a financial instrument", recommending that, for that purpose, the European Securities and Markets Authority (ESMA) is tasked by the Commission with publishing "guidelines in order to reduce legal uncertainty and guarantee a level playing field for market operators": ESC Report, note 61, Recital 2a.

72 Council final compromise text, note 64, Art. 2 para. 3 *litt.* c-k and Recital 3.

73 *Ibid.*, Recital 6.

74 European Securities and Markets Authority (ESMA), *Advice: Initial Coin Offerings and Crypto-Assets*, 2019, p. 19 par. 80, [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf], Accessed 28 February 2023. *Contra* Cassazione Penale (Sez. II), 30 November 2021, No. 44337 (unpublished)

75 Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, [2023] OJ L 150: see Titles II, III, IV and Art. 3 para. 1 n 5.

assets and crypto-asset service providers", the EU legislator, on one hand, has taken the stance that crypto-assets with "no identifiable issuer… should not fall within the scope of Title II, III or IV" of the Regulation, and, on the other hand, that, in any case, crypto-asset service providers providing services in respect of (also) such crypto-assets should be covered by the Regulation, unless… said services are provided in a fully decentralised manner without any intermediary (recital 22).

Nevertheless, the aforesaid, intricated, exceptions and counter-exceptions, mainly aimed at including or excluding certain cryptoassets and management systems from the regulatory perimeter of the MiCA Regulation, are not per se binding, when it comes to defining the scope of the current or future conflict-of-laws regime for cryptocurrencies, and namely for property aspects of the same. Quite the contrary, said exceptions seem to be adding arguments to the autonomous characterization of pure cryptocurrencies as a distinct category from other cryptoassets (and more in general digital assets) that actually embody claims, as well as to their separate private international law treatment.

Although the opposite view, that cryptocurrencies may well embody claims, has also been sometimes maintained both with regard to bitcoins[76] and to Libra Coins,[77] recently re-nominated Diem Coins,[78] what is more relevant here is that, if a general conflict-of-laws regime for crypto assets is to be conceived, any legislative policy option (and, namely, any connecting factor) based on the idea that a claim is embedded in those assets should be tested in respect of its application to "pure" cryptocurrencies.

Along the same line, the Consultation and call for evidence on "Future financial services regulatory regime for cryptoassets" launched by UK HM Treasury in February 2023, despite replacing the term "cryptocurrencies" with the more neutral "exchange tokens", identifies as a distinctive feature of said tokens, as opposed to "security" or "utility" tokens, the fact that they "do not provide the types of rights or access" provided by the latter tokens.[79]

---

[76] *Cf.* Low, K. F. K., *Bitcoins as Property: Welcome Clarity?*, Law Quarterly Review, Vol. 136, No. 3, 2020, p. 345, criticizing the court's findings in *AA*, *op. cit.*, note 28, that bitcoins are an intangible property but not a chose in action.

[77] d'Ornano, A., *Sur le projet Libra*, Revue critique de droit international privé, 2020, pp. 179 ff. The description of the original features of the Libra system and coins may be found in the historical White Paper at [https://sls.gmu.edu/pfrt/wp-content/uploads/sites/54/2020/02/LibraWhitePaper_en_US-Rev0723.pdf], Accessed 28 February 2023.

[78] See the website of the Diem Association, *Welcome to the Diem project*, [https://www.diem.com/en-us/], Accessed, 28 February 2023.

[79] HM Treasury, *Consultation and call for evidence on "Future financial services regulatory regime for cryptoassets"*, 2023, p. 16, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/

However, although the aforesaid distinction might be of relevance to identify the most suitable connecting factors, it is hardly deniable that, once it is acknowledged that cryptocurrencies may be regarded as store of value – purely notional or linked to the value of a fiat currency –, and are susceptible to be transferred and traded,[80] on one hand, it may well be that exclusive rights are asserted over them and that a law regards those claims as worthy of protection against conflicting or competing interests of other parties. On the other hand, it is also hardly deniable that the transfers of cryptocurrencies which take place through the blockchain represent the implementation of a transaction of whichever nature.

Overall, the definition of cryptocurrencies as purely *de facto* assets – that do not incorporate, nor represent, claims, but because of their (notional) value may be the object of transactions – seems sufficient to call for a specific conflict-of-laws analysis.

2.2.2. The Knowledge of the Private Key as (the only) Basis for Control over Cryptocurrencies

In at least apparent contrast to the above, with a view to reconciling the autonomy and immutability of blockchain transfers with the requirement of private justice, a very thorough theory has been recently developed according to which, since the power of the holder of bitcoins resides in his/her knowledge of the private key (that allows him to initiate the transfer to the address, *i.e.*, the public key, of the recipient),[81] one should accept the record on the blockchain as a fact that reveals

attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf], Accessed 28 February 2023.

80 Solinas, M., *Investors' Rights in (Crypto) Custodial Holdings: Ruscoe v Cryptopia Ltd (in Liquidation*), Modern Law Review, Vol. 84 No.1, 2021, p. 160.

81 In the Bitcoin system, users are represented by addresses, which can be regarded as being like a bank account number. An example of a Bitcoin address is a string of letters and numbers (*e.g.*, 3PtFPuXZxS1CBHdG2E5EeU6FcFqGGmzepF). In this way, Bitcoin accounts are pseudonymous. Addresses are created using public key cryptography. The owner of the address is the holder of the private key that corresponds to the public key that has been used to create the address. Therefore, the private key is the proof that a specific address belongs to this user. As a result, private keys must be protected, as their loss means loss of proof that this address belongs to the user and, as a direct consequence, the inability to use the bitcoins in the corresponding accounts. As Bitcoin is not controlled by an entity, it is impossible to claim missing private keys. Addresses are used to hold bitcoins; a user is usually the holder of many addresses. There is no limit on how many addresses a user can have; rather, it is advised to use a new address when receiving bitcoins rather than reusing addresses. This makes the tracking of addresses and linking them to the owners more difficult. To perform a transaction – for example, Alice wants to send 20 bitcoins (BTC) to Bob – Alice will have to prove that she is the owner of an account or a number of accounts that hold at least 20 BTCs. She does this by digitally signing the transaction with the private keys of these accounts. Once signed, rather than being sent directly to Bob, the transaction is broadcast on the whole Bitcoin network. Alice's transaction is pending until a special entity

the current holder of the bitcoin and creates a legal presumption of him being the legitimate holder of that crypto asset (unless it can be proven that the crypto asset has been obtained illegally).[82] Therefore, the law should regard that transfer as immutable and "substitute a conceptualization of the transfer in terms of property law by an analysis that is based on remedies under the law of obligations."[83] Accordingly, in case of mistakes or *exceptio inadimplendi*, the transferor should rely on the "reverse transfer," *i.e.* on the possibility for the law to impose an obligation on the recipient of the crypto asset to return it, whilst, exceptionally, in cases of hacking, blackmail or fraud the transaction could be invalidated.[84] It might be, further, worth considering that, according to that theory, the factual position – *i.e.* the knowledge or, otherwise said, the possession – of the private key is seen as legally protected by way of the applicable tort, contract or security law.[85]

Although the aforesaid approach looks very promising, given the intrinsically cross-border nature of DLT, enacting the premise of such an approach – namely, the aforesaid legal presumption – would entail the general acceptance, either through the adoption of a single international instrument providing for uniform substantive rules or via parallel pieces of national legislation, of the aforementioned legal presumption. For the moment, however, the first stance taken by national lawmakers and case-law seems rather inclined to frame bitcoins into more traditional patterns of property law.

Be that as it may, the aforesaid theory has (also) the merit of drawing attention to the *de facto* situation connected with the knowledge of the private key. In the same vein, the UNIDROIT Working Group on Digital Assets and Private Law, while elaborating a set of Principles to support States in adopting substantive and conflict-of-laws rules on digital assets, under Principle 6, has identified that situation with the term "control" and clarified that "a person has 'control' of a digital

in Bitcoin, known as a "miner," verifies it. The miners collect pending transactions, then confirm their correctness before verifying them. To summarize, Alice wants to send 20 BTC to Bob. The closest sum of her addresses to the targeted amount is 21.1 BTC. The transaction is broadcast on the Bitcoin network and once verified, Bob receives the 20 BTC, the miner receives 0.1 BTC as a transaction fee, and 1 BTC is returned to Alice as change. Once the transactions have been verified, they are stored in a tamper-resistant and shared data structure comprising of a list of blocks which are chained together, known as a blockchain. New transactions are inserted into a block at the end of the chain and linked to the previous block of transactions, as each block references the previous block's hash.

82 Lehmann, M., *Who Owns Bitcoin? Private Law Facing the Blockchain*, Minnesota Journal of Law, Science & Technology, Vol. 21, No. 1, 2019, pp. 119-120.

83 *Ibid*., p. 123. The approach as above is aknowledged in *Tulip Trading Ltd v Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch) (3 February 2023), esp. paras. 83-84.

84 *Ibid*., paras. 128-30.

85 *Ibid*., par. 128.

asset if: (a) …the digital asset or the relevant protocol or system confers on that person: (i) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; (ii) the ability to obtain substantially all the benefit from the digital asset; and (iii) the exclusive ability to transfer the abilities in sub-paragraphs (a)(i), (a)(ii) and (a)(iii) to another person (a 'change of control'). (b) the digital asset, or the relevant protocols or system, allows the person to identify itself as having" those abilities. [86] What is more relevant here is, first, that, according to the Commentary to those Principles, the "'control' assumes a role that is a functional equivalent to that of 'possession' of movables," insofar as in the markets for digital assets, those who acquire control over the assets "expect and believe" that they have obtained, through control, the relevant exclusive abilities,[87] and, second, that, for the purpose of the identification requirement set forth under (b), "an identifying number, a cryptographic key, an office, or an account number" may be, "by a reasonable means", of relevance, "even if the means of identification does not indicate the name or identity of the person to be identified."[88] Moreover, the relevance of the "exclusive ability" requirements for the purpose of said Principles as "an inherent aspect of proprietary rights" acknowledges the tendency to frame the relationship between users and digital assets in terms of property rights.[89]

Therefore, the following section will investigate the PIL regime of proprietary aspects of cryptocurrencies.

3. THE PIL REGIME OF CRYPTOCURRENCIES AS "PROPERTY"

Looking at the role played by cryptocurrencies as a store of value, according to the traditional pattern in property matters, it is for the law governing property rights, as determined through the relevant conflict-of-laws provision – in principle the *lex situs* –, to establish whether a specific "thing" can be the subject matter of property rights, the classification of that thing as immovable or movable (or else), as well

---

86 UNIDROIT, *Principles on Digital Assets and Private Law*, as approved by the Governing Council at its 102th session, Rome, 10-12 May 2023, C.D, (102), 2023, pp. 38-41, [https://www.unidroit.org/wp-content/uploads/2023/04/C.D.-102-6-Principles-on-Digital-Assets-and-Private-Law.pdf], Accessed 19 July 2023.

87 *Ibid*., 38 para. 6.1-6.3.

88 *Ibid*., 42 Principle 7(2).

89 *Ibid*., 38 para. 6.1. On the other hand, the recently adopted *ELI Principles on the use of Digital Assets as a Security*, [https://www.europeanlawinstitute.eu/projects-publications/completed-projects/use-of-digital-assets-as-security/], Accessed 28 February 2023, seems to envisage a mixed approach as regards the definition of "control", referring either to "the legal power or factual capability of any natural or legal person to deal in and/or extinguish such assets, as the case may be".

as the types and contents of those rights, *i.e.* the prerogatives of the person who "holds" the thing. When it comes to intangible assets, and especially, digital assets, however, the effectiveness of such a paradigm is largely put to the test, first and foremost, due to the difficulty, or rather impossibility, to identify a physical location for them, though not only because of that objective issue. Conversely, with regard to intangible assets incorporating claims, the further specificities, both in terms of notion of property rights and of applicable connecting factors, lie in the fact that the asset *is* the relationship with the debtor, which has its own governing law.

Once it is generally accepted that the factual relationship between a cryptocurrency and its holder entails that the latter has the exclusive ability to dispose of the former and to exclude others from the benefits thereof and that accordingly such relationship may be construed as property, the applicable law will determine the conditions upon which a person has a proprietary right in a cryptocurrency and that right may be validly transferred,[90] including the rules for the original acquisition of title (*e.g.* the possibility to invoke the defences of good faith purchase for value)[91] and the derivative transfer of title (generally, either through party's consent or delivery of the asset), as well as any requirements regarding time of perfection, publicity,[92] need for specification,[93] and the realisation of the right over the asset,[94] both having regard to the rights as between the transferor and the transferee *inter se*, and to the legal consequences of the transfer *vis-à-vis* third parties,[95] including the transferor's creditors.[96] As unlikely as it might seem because of the validation mechanisms embedded in the blockchain systems, which are precisely aimed at preventing any double transfer of the same token, the same law will govern the priority of the rights among competing transferees of the same token. Moreover,

---

90 Lehmann, *op. cit.*, note 10, p. 150.

91 Fox, *op. cit.*, note 26, para. 6.57 ff.

92 Carr, *op. cit.*, note 25, paras. 7.18-7.20.

93 *Ibid.*, paras. 7.16-7.17.

94 Financial Markets Law Committee, *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*, 2018, p. 11 para. 4.7, [http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf], Accessed 28 February 2023.

95 Although UNIDROIT Principles, *op. cit.*, note 80, p. 23, include "the legal consequences of third-party effectiveness of a transfer of a digital asset" and "the requirements for, and legal consequences of, third-party effectiveness of a security right in a digital asset" among matters governed by "other law" (*cf* Principle 3(3)), it seems that the conflict of laws provisions set forth in Principle 5 cover "proprietary issues", without exceptions (*cf* para. 5.2, p. 33).

96 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims - General approach (9050/21), 28 May 2021, art 5 *litt*. c.

the same law will establish the forms of security that may be validly granted over the cryptocurrency.[97]

It is now time to explore some policy options for a conflict-of-laws regime for said property aspects of cryptocurrencies.

First and foremost, among the solutions that have been so far envisaged by scholars and think-tanks for crypto assets, the approach which favours the application of the law under which the right/claim represented by the crypto asset, as admitted by its own promoters,[98] cannot apply to intrinsic tokens, such as "pure" cryptocurrencies. In fact, as anticipated, cryptocurrencies do not represent nor incorporate rights.[99] The same goes for any approach centered around the issuer of the crypto assets, since cryptocurrencies do not embed a claim against an issuer, whereas the original coder does not undertake any obligation towards the subsequent transferees of the assets.[100]

The absence of any underlying claim, coupled with the inherent nature of "pure" cryptocurrencies as items representing value, albeit a notional and volatile one, would, thus, locate their conflict-of laws regime into the realm of the *lex rei sitae* principle. This is premised (also) on the need for "an objective and easily ascertainable connecting factor to which third parties might reasonably look to ascertain questions of title," which represents the first component of the rationale underlying the application of that principle in property matters[101] and is even more

---

97 UK Jurisdiction Taskforce, *op. cit.*, note 28, p. 25; ISDA, McCann FitsGerald; r3, *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Irish Law*, 2020, p. 29, [https://www.isda.org/a/ACrTE/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-Irish-Law.pdf], Accessed 28 February 2023.

98 Takahashi, K., *Blockchain-based Negotiable Instruments (with Particular Reference to Bills of Lading and Investment Securities)*, SSRN, 2021, para. 5.6.3, [https://ssrn.com/abstract=3937664], Accessed 28 February 2023.

99 Financial Markets Law Committee, *op. cit.*, note 90, 20 para. 6.27; Ng, M.*, Choice of law for property issues regarding Bitcoin under English law*, Journal of Private International Law, Vol. 15, No. 1, 2019, p. 315.

100 European Parliament resolution of 8 October 2020, *op. cit.*, note 4, Recital AN; Annunziata, F., *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offering*, European Company and Financial Law Review, Vol. 17, No. 2, 2020, pp. 150-153; ISDA, Jones Day; and r3, *"Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: French Law"*, 2020, p. 19, [https://www.isda.org/a/ZCrTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT-French-Law.pdf], Accessed 28 February 2023.

101 Collins, Lord of Mapesbury; Harris, J. (eds.), *Dicey, Morris & Collins on the Conflict of Laws*, 16th edn, London, 2022, para. 22-025.

relevant for assets that could be used by companies to obtain liquidity and have access to credit through collateralisation.[102]

However, the aforementioned technical features of cryptocurrencies, which originate in and are transferred through a ledger system that is dematerialised and distributed, make the application of the situs principle, at least in its traditional form, impossible in practice and unsuitable for the second limb of its rationale, which lies in the fact that "the country of the *situs* has control over the property and a judgment in conflict with the *lex situs* will often be ineffective,"[103] since the actual possibility for an authority to have any form of control over crypto assets, including to enforce any regulation, should rely on different grounds. Nevertheless, both limbs of that rationale should be included in the parameters against which to test the soundness of any conflict-of laws regime for cryptocurrencies too, besides those related to the foreseeable use-cases of those assets.

In that regard, the need to find appropriate PIL solutions is reinforced by the pattern of disintermediation that is (or should be) intrinsic to DLT ecosystems by virtue of the traceability and collective validation of transactions taking place in and through those ecosystems. Disintermediation should *per se* rule out the possibility to envisage conflict-of-laws rules modelled on the ones related to book-entry securities that are based on the location of the relevant intermediary. Nevertheless, the current practice reveals that the prevailing framework for cryptocurrencies has become an indirect holding pattern, characterized by a combination of two-tier networks based on a distributed and decentralized scheme where the nodes are often represented by exchanges, *i.e.* crypto asset service providers in the language of the proposed EU Regulation on Markets in Crypto-assets,[104] that are connected to the adjacent nodes within the blockchain (*i.e.* a distributed network) and where additional nodes are also formed among investors in cryptocurrencies at the level of the relevant exchanges (*i.e.* a decentralized network).[105] Such practice may neither affect the technical features of the cryptocurrencies' holding and transfer schemes, as far as the exchanges/intermediaries' holding pattern applies the same schemes, nor, accordingly, the need to have legislative solutions well aligned with technology, but may have relevance when testing any legislative option against the substantive interests and aptitudes of the end-users, In fact, it might turn out that more often than expected, DLT end-users are professional operators.

---

102 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM(2018) 96 final, p. 2.

103 Collins; Harris, *op. cit.*, note 97, para. 22-025

104 Council final compromise text, *op. cit.*, note 64, Art. 3 para. 1 n 9.

105 Solinas, *op. cit.*, note 76, p. 156.

Furthermore, a basic theoretical question (with relevant practical consequences) should be considered. Conceptualizing the relationship between persons and cryptocurrencies in terms of property rights entails a generalized acceptance of the preliminary proposition(s) that (i) a notional value is worthy of being regarded as the subject matter of property rights, and (ii) the transfer of that value, *i.e.* the cryptocurrencies, according to the technical requirements of DLTs, implies a transfer of property right(s) over that value or, in other words, that a transfer of cryptocurrencies through the system is a legally sound way to dispose of said assets. However, this second proposition does not necessarily mean that a "transfer" within the system from which cryptocurrencies derive their existence is the only way to "dispose of" property rights over the same, unless a law establishes that it is so in terms of conditions for the validity of the transfer and opposability of the same against third parties. The last question is particularly relevant when it comes to investigating desirable conflict-of-laws approaches (and, particularly, about connecting factors) and the (possible) need to take into account both on-chain and off-chain acts of disposition for that purpose. In that regard, the business practice may, of course, offer some very much useful data to construct some answers, but the final say rests with the relevant applicable law, …which leads to a kind of circular argument.

However, as advanced above,[106] an alternative theory has suggested that the proposition under (i) is replaced by a "protection by private law" that goes "beyond traditional conceptions of property in physical objects" and is "independent of any showing of legal title," whereby "the mere factual situation that the private key was created for some person should suffice as a basis for claim of return"[107] and for the recognition of "some form of legal status" that is "also necessary for the creation of a security right over the crypto asset" in question. The same doctrine has further argued that it could be left "to the applicable tort, contract, or security law" to "call" that status as "property" or "possession" or "by another term,"[108] as well as to protect it through the relevant remedy.[109]

In-between stands, so to say, a third approach, which does not give up on characterizing cryptocurrencies – or, rather, the "factual" benefit accruing to a person as a participant to a cryptocurrency system (the value of which relies upon "a legitimate expectation, founded on the technological features of the system, that

---

106 *Supra* para. 2.2.2.

107 Lehmann, *op. cit.*, note 78, p. 128.

108 *Ibid.*, pp. 127-128.

109 For a similar critique of the adoption of the "Physical Model" to frame the relationship between persons and intangible assets in the wake of the advent of the electronic era see Benjamin, J., *Interests in Securities: A Proprietary Law Analysis of the International Securities Markets*, Oxford, 2000, pp. 303 ff.

the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system") – as "a form of intangible property within the conflict-of-laws."[110] Yet, a distinction is made between "internal effects" of transactions within a cryptocurrencies system, which should be resolved by reference to the system's consensus rules and any law applicable by virtue of the relevant conflict-of-laws rules concerning contractual obligations,[111] on one hand, and the "external effects," to which separate choice of law rules apply, on the other. At the same time, however, this doctrine admits that the proprietary character of a cryptocurrency "depends" on relationships within the system,[112] illustrating that proposition through the case of parties wishing to create a security interest over units of a cryptocurrency. To this end, said parties may, or may not, enter into an arrangement which involves a transaction within the blockchain initiated by the grantor for the benefit of the grantee. In the second scenario the creation of the security may entail, for instance, that the grantor gives the grantee control over or access to a cryptocurrency wallet. In the first scenario, instead, the initiation of a transaction within the DLT system would engage "the separate relationships of the grantor, grantee, and many others as participants in the system."[113] By way of further example, it is mentioned that, if, for some technical reasons, the transaction within the system is ineffective, the grantee may need to rely on a proprietary entitlement existing outside the system. Also, if the transaction within the system is successfully validated but the system lacks the technical possibility to re-vest the cryptocurrency in the grantor upon redemption, the grantor may benefit from the protection afforded by the "external" proprietary entitlement. By the way, the aforesaid examples seem to provide support to the conceptualisation of cryptocurrencies holding pattern in terms of property rights, while, at the same time, demonstrating the relevance of and the need for "external" legal remedies to enforce those rights.

4. AVAILABLE OPTIONS FOR A CONFLICT-OF-LAWS REGIME

In going over the various possible approaches to determine the law applicable to "pure" cryptocurrencies, first, certain objective connecting factors that are pegged

---

110 Dickinson, *op. cit.*, note 55, p. 127 para. 5.97; Steinrötter, B., *International Jurisdiction and Applicable Law*, in: Maume, P.; Maute, L.; Fromberger, M. (eds.), The Law of Crypto Assets. A Handbook, München, Oxford and Baden-Baden, 2022, pp. 75 f.

111 *Ibid*., pp. 106 ff.

112 *Ibid*., p. 127 para. 5.95.

113 *Ibid*., p. 127 para. 5.94.

to the ecosystem in which cryptocurrencies originate and are transferred will be considered, then, some propositions centered around the transferor and/or the transferee will be addressed, and, finally, schemes based on party autonomy will be explored.

4.1. The "PROPA" and "PREMA" criteria

A first batch of proposals looks to the place of the relevant operating authority or administrator ("PROPA"),[114] either in form of objective connecting factor[115] or by empowering that authority to establish the applicable law. The significance of that connection would be, of course, particularly relevant in case of an operator which is registered and supervised under some national law.[116] Both versions, indeed, reflect the wish for a single law to govern all aspects of transactions within the system.[117] Such an approach presupposes that the relevant DLT system is permissioned and not decentralised,[118] with a single entity performing core functions, such as management activities, and acting as a point of contact and a gatekeeper on behalf of the regulators. Moreover, the enactment of a rule grounded on PROPA would, in any case, require a clarification of the actual role of the "relevant administrator," by specifying the activities which represent the essence of that role and a threshold of "relevance," especially in cases where the entity in question only performs limited functions, such as providing technical access to the system, or where there are two (or more) entities performing similar functions located in different states.[119] However, PROPA seems unable to work for permissionless/public systems like Bitcoin.

The same rationale would underlie an approach based on the location of the original coder of the DLT system or the private master key for the same (usually the

---

114 In the opinion of the UK Jurisdiction Taskforce, *op. cit.*, note 28, p. 99, in determining whether English and Welsh law governs the proprietary aspects of dealings in crypto assets, one of the factors that might be "particularly relevant" is whether there is any centralized control in England and Wales.

115 Gesetz über elektronische Wertpapiere (eWpG), *op. cit.*, note 43, § 32 "1. Unless § 17a of the Custody Account Act applies, rights in an electronic security and dispositions of an electronic security shall be governed by the law of the state under whose supervision the register-keeping entity in whose electronic securities register the security is registered is located. 2. If the entity keeping the register is not under supervision, the registered office of the entity keeping the register shall be decisive. If the registered office of the entity keeping the register cannot be determined, the registered office of the issuer of the electronic security shall be decisive" (unofficial translation).

116 Lehmann, *op. cit.*, note 10, p. 169.

117 Ooi, M., *Choice of Law in the Shifting Sands of Securities Trading*, in: Dickinson A.; Peel, E. (eds.), A Conflict of Laws Companion. Essays in Honour of Adrian Briggs, Oxford, 2021, p. 213.

118 de Vauplane, H., *Blockchain And Conflict of Laws*, Revue Trimestrielle de Droit Financier, 2017, p. 52.

119 Financial Markets Law Committee, *op. cit.*, note 91, p. 18 paras. 6.16-6.17.

primary residence of the keyholder; hence the acronym "PREMA"), that is the key by which the relevant operator or administrator is enabled to control all transfer of assets within the system, in that such master key is used to encrypt and store all other keys in the system. In either cases, besides the costs to market participants of ascertaining the location of these entities, one may question why the original coder should affect the ongoing life of the system (and all the transactions therein executed), especially where (s)he is not also the system administrator.

4.2. The Transferor's or the Transferee's Location

A second group of theories looks to the location of the parties to the transactions, either in the form of their habitual residence (or centre of main interest or domicile) or of their private encryption key (or of the wallet where private keys are stored).[120]

The solutions based on the transferor mirror the approach undertaken in the latest available text of the Proposal for Regulation on the law applicable to third party effects of assignment of claims (*per se* not applicable to the third party effects of the transfer of crypto assets)[121] as a general rule.[122] In both frameworks, the main advantage of said criterion has been identified in the convenience it brings to the transfer of claims/assets in bulk, in that all the claims/assets held by the transferor-assignor-borrower become subject to the same law with regard to third party effect

---

120 This approach is supported by de Vauplane, *op. cit.*, note 114, p. 50 and Green, S.; Snagg, F., *Intermediated Securities and Distributed Ledger Technology*, in: Gullifer, L.; Payne, J. (eds.), Intermediation and Beyond, Oxford, 2019, p. 357, based on the analogy with traditional bearer securities. The UK Jurisdiction Taskforce, *op. cit.*, note 28, p. 99, qualifies as "particularly relevant" also "whether a particular crypto asset is controlled by particular participant in England and Wales because, for example, a private key is stored here".

121 Council of the European Union, *op. cit.*, note 92, Art. 1 para. 1ab. Conversely, pursuant to Art. 4 para. 2 of the same Proposal, "[t]he law applicable to the assigned claim shall govern the third-party effects of the assignment of: … (ba) claims arising out of crypto-assets that do not qualify as financial instruments or electronic money." See also Recital 16bis and Recital 27bis. According to Recital 16bis, last sentence, "[i]n order to avoid characterisation problems as to whether a certain crypto-asset qualifies as a financial instrument or another type of crypto-asset, claims arising from all crypto-assets should be covered by th[e] Regulation, with the exception of claims arising out of crypto-assets that qualify as transferable securities, money-market instruments or units in a collective investment undertaking." That provision will, of course, apply to all crypto assets capable of giving rise to "claims" according to the definition provided in Art. 2 *litt*. d, *i.e.*, "the right to claim a debt of whatever nature, whether monetary or non- monetary, and whether arising out of a contractual or a non-contractual obligation." It is worth noting that Art. 2 *litt*. hc and Recital 16bis of the Proposal expressly refer to the definition of "crypto-asset" "as defined" in the relevant provision of the MiCa Proposal, *op. cit.*, note 60.

122 Council of the European Union, *op. cit.*, note 92, Art. 4 para. 1.

of the transfer-assignment.[123] Moreover, that criterion offers the additional advantage that it does not put the transferee-financier in a more favourable position than other possible competing claimants seeking to challenge the transfer.

On the other hand, the solutions based on the location of the transferee (or of her private key) mirror the PRIMA principle embodied in the FCD[124] and, with certain differences, in the Hague Securities Convention,[125] where the relevant factor is also in the control of the transferee, *i.e.* the financier, who, therefore, is allowed to ascertain the applicable law much more easily and before anyone else.[126] Moreover, the main advantage of the transferee/current holder rule has been identified in that it applies the law of the state which can effectively enforce any judgment.[127]

More in general, as advocated in the last edition of *Dicey, Morris*,[128] the location of the owner is reasonably objectively identifiable. In addition, even though direct control over a cryptocurrency might be beyond any individual state, the owner of the cryptocurrency has control over the property, generally through their control over the private encryption key which is required to transfer the property, and the state of location of the owner thereby has the strongest indirect control over the property. Along the same line, the "owner" should generally be understood to refer to the party in possession of the private encryption key giving access to the cryptocurrency at the time of the relevant transaction.[129] If an encryption key is duplicated, the "owner" should generally be understood as the party who in fact exercises control over the cryptocurrency, for example, through effecting a sale to a third party. In case of hacking, the owner's residence or place of business[130] at the time of the hack or misappropriation would be of relevance,[131] whilst the location of its servers are regarded as "an adventitious circumstance".[132]

---

123 Ooi, *op. cit.*, note 113, p. 216.

124 Directive 2002/47/EC of the European Parliament and of the Council on financial collateral arrangements [2002] OJ L168/43, Art. 9.

125 Hague Conference on Private International Law, Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, Art. 4.

126 The same line of reasoning is supported by J. Pelling in *Osbourne v Persons Unknown & Anor* [2022] EWHC 1021 (Comm) (10 March 2022) in cases relating to crypto currency fraud "crypto assets, are to be treated as located at the place where the owner of them is domiciled".

127 Ng, *op. cit.*, note 95, p. 335.

128 Collins, Harris, *op. cit.*, note 97, para. 23-050.

129 *Tulip Trading Ltd v Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch) (25 March 2022), 148.

130 *Ibid.*, 149.

131 *D'Aloia v Person Unknown & Ors* [2022] EWHC 1723 (Ch) (24 June 2022), 10.

132 *LMN v Bitflyer Holdings Inc & Ors* [2022] EWHC 2954 (Comm) (29 November 2022), 20.

However, against approaches based on the transferor's or transferee's location the following critiques have been raised: the blockchain becomes subject to as many laws as the number of states where the users or their private keys are located, the identity of users is often unknown (or difficult to trace) and, accordingly, it is difficult to identify the place of the private key.[133] Moreover, the private key is a code that may or may not be associated with any particular tangible device which generates it or stores it.[134] An additional significant disadvantage of the criteria based on the transferor's location would be that they would often provide unclear answer to questions of entitlement in cases of joint transferors or a change in the transferor's habitual residence or domicile.[135]

The same objections have been raised against another doctrine, likewise centered on the transferor's location. In fact, building upon the analogy between the factual benefit accruing to a person as participant in the blockchain and the goodwill of a business, which in English conflict-of-laws is equally qualified as a species of intangible property, it is argued that "proprietary effects outside the cryptocurrency system of a transaction relating to cryptocurrency shall in general be governed by the law of the country where the participant resides or carries on business at the relevant time."[136] In case that the relevant user resides or carries on business in more than one state at that time, the relevant place would be the place of residence or business of the user "with which the participation [in the cryptocurrency] that is the object of the transaction is most closely connected."[137] The emphasis on the effects of transactions outside the cryptocurrencies system, on one hand, allows that doctrine to highlight the predictability and ease of application in comparison with other possible choice of law approaches, as well as the close alignment with

---

133 Audit, M., *Le droit international privé confronté à la blockchain*, Revue critique de droit international privé, 2020, para. I.B; Ooi, *op. cit.*, note 113, p. 215.

134 Ooi, *op. cit.*, note 113, p. 215.

135 Financial Markets Law Committee, *op. cit.*, note 90, p. 20 para. 6.22.

136 This approach has been applied in *Ion Science & Duncan Johns, op. cit.,* note 29, 13, whereby, as reported by Sleave, *op. cit.*, note 29, English law was found to apply, as England was the place where the damage occurred. This was on the basis that Mr. Johns' bank account was an English account, or that the funds were taken from the applicants' control in England, because either Mr. Johns' computer was in England, or because the relevant bitcoin was located in England prior to the transfer. As to the latter point, this was said to be because the *lex situs* of a crypto asset is the place where the person or company who owns it is domiciled, although Mr. Justice Butcher acknowledged there is no decided case on this point and relied on textbook authorities (which, incidentally, has been identified with Andrew Dickinson in the following online posting: Moir A. *et al*, *High Court considers where cryptocurrencies are located and compels disclosure of information by cryptocurrency exchanges outside the UK*, Herbert Smith Freehills, 2021, [https://hsfnotes.com/litigation/2021/02/24/high-court-considers-where-cryptocurrencies-are-located-and-compels-disclosure-of-information-by-cryptocurrency-exchanges-outside-the-uk/], Accessed 28 February 2023.

137 Dickinson, *op. cit.*, note 55, p. 132 para. 5.109.

the rules that apply to cross-border insolvency.[138] On the other hand, the distinction between the external effects, governed by the law of the state of the transferor's residence or business, and the internal effects, tentatively attributed by this doctrine to the law governing the (contractual) relationship between participants in the system, would allow the assertion of proprietary rights based on the law applicable to "external effects" against another user who, after being granted "externally" with security interests in a cryptocurrency, uses the information provided to him by the owner of the cryptocurrency (and grantor of the security interest) to initiate an irreversible transaction within the system in favour of a third party. One may reply that distinguishing between external and internal proprietary effects for the purpose of identifying the applicable law creates exposure to misalignments, for instance, in the substantive requirements for the opposability of property rights, thereby paving the way for inextricable conflicts of competing assertions of proprietary rights on the part of different persons. While advocating for uniform substantive rules, especially on this aspect, one should not overrate the actual impact of such misalignments, keeping in mind that the existence of different proprietary rights, each governed by a different law, is a very common pattern in the framework of proprietary rights over intermediated securities.[139] Yet, an additional warning is to be given about the need to have in place some kind of settlement regime, capable of (i) combining coherently both the external and the internal proprietary effects of transactions over cryptocurrencies, and (ii) counterbalancing the lack of deterministic operational finality of said transactions[140] with legal mechanisms to define the moment(s) of settlement finality.[141]

---

138 *Ibid*., pp. 132-133 para. 5.110.

139 See Dixon, V., *The Legal Nature of Intermediated Securities: An Insurmountable obstacle to Legal Certainty?*, in: Gullifer, L; Payne, J. (eds.), Intermediation and Beyond, Oxford, 2019, pp. 70 ff, for a detailed analysis of that pattern in cross-border settings.

140 The finality of payments and settlements on the Bitcoin blockchain is viewed as probabilistic due to the likelihood that the most recent transactions embedded in the blockchain may be undone or bitcoins may be double spent due to a formation of a fork: see Bank for International Settlements, *Annual Economic Report*, 2018, pp. 101-104, [https://www.bis.org/publ/arpdf/ar2018e.htm], Accessed 28 February 2023. However, the same applies to the operational settlement with cash and any other means of electronic payments, as there is always a theoretical possibility of taking the cash back by using brute force or reversing the transaction due to a technical failure in the payment system, including that of a central bank.

141 The need for (and the difficulties linked to) the establishment of a regime capable of providing legal finality in Proof-of-Work blockchains are pointed out by Nabilou, H., *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, SSRN, 2022, [http://dx.doi.org/10.2139/ssrn.4022676], Accessed 28 February 2023. On this topic see also Committee on Payments and Market Infrastructures, *Distributed ledger technology in payment, clearing and settlement: An analytical framework*, BIS, 2017, [https://www.bis.org/cpmi/publ/d157.pdf], Accessed 28 February 2023; Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments, *The use of DLT in post-trade processes*, ECB, 2021, [https://www.ecb.europa.eu/pub/pdf/other/ecb.20210412_useofdlt-

4.3. The Elective *Situs/Lex creationis* Approach…

The intrinsic connection between "pure" cryptocurrencies and the system in which they originate and through which they are transferred is, instead, at the core of the approach which looks to the law governing the system, alternatively, as the "*situs*" of the assets or the *lex creationis*, *i.e.* the law of the system by which cryptocurrencies are created.[142] In either case, the law applicable to the system is identified with the law agreed to by participants to the system (the originator and the nodes) either explicitly or implicitly by dealing with crypto assets within the system.[143] The same rationale underlies the reference made in the new UCC art 12 to "the controllable electronic record itself, records attached thereto or associated therewith", as an alternative to "the system in which the controllable electronic record is recorded", that "determines the controllable electronic record's jurisdiction and, thereby, the governing law".[144] Even more explicitly, Principle 5 of the Draft UNIDROIT Principles on Digital Assets and Private Law provides that "proprietary issues in respect of a digital assets are governed by… the domestic law of the state… expressly specified in the digital asset as the law applicable to such issues" or, lacking such indication, "in the system or platform on which the digital asset is recorded". [145]

The advantages of the approach centered around the system, sometimes referred to as the "elective situs" following the model of the "contractual PRIMA" which labels the Hague Securities Convention, is said to lie in the fact that the effects of all the transactions within the system are governed by the same law and that participants in the system cannot complain about the application of that law since it is the law to which they have submitted, which, moreover, has the most significant connection with the crypto assets, and especially native tokens. Moreover, the law governing the system is said to be easily ascertainable both by parties to each transaction, as well as by third parties, themselves likely to be participant in the same system. The main obstacles to the elective *situs/lex creationis* approach lie, on one hand, in the possible reluctance to see the effects of a choice-of-law agreement extended to third parties who do not participate in the relevant system, and, on the other hand, in possible concerns regarding the risk of circumvention of regulatory requirements or related to the choice of a law which might be subject to undue external or private influence. The former concerns could, however, be, at

---

posttradeprocesses~958e3af1c8.en.pdf?2779d0668b55434a0e67174b3f1183a4], Accessed 28 February 2023.

142 Ooi, *op. cit.*, note 113, pp. 220-221.

143 *Ibid.*, p. 219.

144 Uniform Commercial Code Amendments (2022), *op. cit.*, note 49, Section 12-107.

145 Draft UNIDROIT Principles on Digital Assets and Private Law, *op. cit.*, note 82.

least partially, mitigated through the requirement of an express designation of the applicable law, thereby drawing everyone's attention on that designation and fostering its visibility, whilst the latter concerns could be addressed by combining the elective *situs* rule with a requirement that the selected law has an objective connection with the system, which could, moreover, be specified through a list of factual elements which should be considered for that purpose. Alternatively, the effectiveness of the choice-of-law agreement could be made conditional upon the approval of the relevant regulatory authority (which would entail, however, the need for the relevant legislative forum to be entitled to adopt both conflict-of-laws and regulatory rules within the same national or international framework). It might be worth noticing, however, that the MiCA Regulation provides that the crypto-asset white paper which, according to Article 4 para 1 litt. b, shall accompany a request for admission of a crypto asset to trading on a trading platform for crypto assets, shall contain, on one hand "the applicable law and the competent court of the offer *and of the crypto-asset*" (Annex I, Part C, n 14; emphasis added), and on the other, "…the following clear and prominent statement on the first page: 'This crypto-asset white paper has not been reviewed or approved by any competent authority in any Member State of the European Union…'" (art 5 para 3).

4.4 …with Some *Addenda*

However, what the elective *situs* approach fails to provide is a solution for systems or assets which lack any agreement as to the applicable law, and this might often be the case for permissionless systems. A comprehensive conflict-of-laws regime for proprietary effects of transactions over cryptocurrencies, based on the elective *situs* and some requirements in terms of objective connection of the selected law, therefore requires a fall-back rule,[146] which should provide different sub-rules for permissioned and permissionless systems. As for the former, the PROPA approach might be a workable solution which, like the main rule, would lead to a single law applicable to the effects of all transactions within the system. For the latter systems, the reasons for having a single law applicable to all transactions seem much weaker and, in any case, it would be very complicated to achieve this goal in light of the aforesaid difficulty to identify a meaningful objective connecting factor for permissionless systems. For those systems, the transferor's habitual residence or registered seat might represent a practical solution, at least for the effects of transaction in cryptocurrencies outside the system, whereby in most cases it should be

[146] In the opinion of Guillame, F., *Blockchain: le pont du droit internatonal privé entre l'espace numérique et l'espace physique*, in: Pretelli, I. (ed.), Conflict of Law in the Maze of Digital Platforms, Cham, 2018, p. 180, in the absence of a valid choice of law agreement, the *lex fori* would be applicable, since any territorial connecting factor would be devoid of any relevance in DLT's settings.

possible to ascertain the identity and the location of the relevant parties. For the proprietary effects of transactions relating to cryptocurrencies within the system, the principle embodied in recital 38 of the Rome I Regulation – according to which the law that applies to the contract between the assignor and assignee under that Regulation "also applies to the property aspects of an assignment, as between assignor and assignee, in legal orders where such aspects are treated separately from the aspects under the law of obligations" might serve as a basis for discussion, at least in case the recently advanced proposition to create a legal identifier of securities for PIL purpose, which would make visible the applicable law as determined under the relevant conflict-of-law rules, will be adopted and extended to crypto assets.[147] However, the most recent attempts to draft a fall-back rule, lacking an elective situs, seem to converge on the lex fori. This is the case of both UCC Section 12-107(d) and UNIDROIT draft Principle 5.

All in all, the elective *situs* approach resonates both with the overall concept of DLTs, as a "space" where party autonomy, as embedded into the digital processes (*i.e.*, the code), creates the assets and handle them, and with the notional value of cryptocurrencies. Yet, the spontaneous process of aggregation underlying the establishment of DLT systems – at least the permissionless ones – calls for fall-back rules, based on objective connecting factors, that pursue predictability of the applicable law. Identifying the relevant party for whom, primarily, predictability should be achieved is only one of the manifold challenges ahead for lawmakers.

REFERENCES

BOOKS AND ARTICLES

1. Anderberg A. *et al.*, *Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, in: Figueiredo Do Nascimento S.; Roque Mendes Pólvora, A. (eds.), Publications Office of the European Union, Luxembourg, 2019
2. Annunziata, F., *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offering*, European Company and Financial Law Review, Vol. 17, No. 2, 2020, pp. 129-154
3. Audit, M., *Le droit international privé confronté à la blockchain*, Revue critique de droit international privé, 2020, pp. 669-696
4. Barsan, I. M., *Legal Challenges of Initial Coin Offerings (ICO)*, Revue Trimestrielle de Droit Financier (RTDF), No. 3, 2017, pp. 54-65
5. Benjamin, J., *Interests in Securities: A Proprietary Law Analysis of the International Securities Markets*, Oxford, 2000

147 Paech, P., *Conflict of Laws and Relational Rights*, in: Gullifer L.; Payne, J. (eds), Intermediation and Beyond, Oxford, 2019, pp. 305-307.

6. Bocchini, R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, Il diritto dell'informazione e dell'informatica, Vol. 33, No. 1, 2017, pp. 27-54
7. Carr, D., *Cryptocurrencies as Property in Civilian and Mixed Legal Systems*, in: Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, pp. 177-198
8. Collins, Lord of Mapesbury; Harris, J. (eds.), *Dicey, Morris & Collins on the Conflict of Laws*, 16th edn, London, 2022
9. Crockett, M., *Wyoming's DIY Project Gets Western with the UCC*, Wyoming Law Review, Vol. 20, No. 1, 2020, pp. 105-148
10. de Vauplane, H., Blockchain And Conflict of Laws, Revue Trimestrielle de Droit Financier, 2017, pp. 50-52
11. Dickinson, A., *Cryptocurrencies and the Conflict of Laws*, Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, pp. 93-138
12. Dixon, V., *The Legal Nature of Intermediated Securities: An Insurmountable obstacle to Legal Certainty?*, in: Gullifer, L; Payne, J. (eds.), Intermediation and Beyond, Oxford, 2019, pp. 47-84
13. d'Ornano, A., *Sur le projet Libra*, Revue critique de droit international privé, 2020, pp. 179-184
14. Fauceglia, D., Scambio e deposito di criptovalute: la responsabilità del gestore della piattaforma, Giurisprudenza italiana, No. 18, 2020, pp. 2659-2666
15. Fauceglia, D., *Il deposito e la restituzione delle criptovalute*, I Contratti, No. 6, 2019, pp. 669-680
16. Finck, M., *Blockchain Regulation and Governance in Europe*, Cambridge, 2018
17. Fox, D., *Cryptocurrencies in the Common Law of Property*, in: Fox D.; Green, S. (eds.), Cryptocurrencies in Public and Private Law, Oxford, 2019, pp. 130-176
18. Green, S.; Snagg, F., *Intermediated Securities and Distributed Ledger Technology*, in: Gullifer, L.; Payne, J. (eds.), Intermediation and Beyond, Oxford, 2019, pp. 337-358
19. Guillame, F., *Blockchain: le pont du droit internatonal privé entre l'espace numérique et l'espace physique*, in: Pretelli, I. (ed.), Conflict of Law in the Maze of Digital Platforms, Cham, 2018, pp. 163-189
20. Haentjens, M.; De Graaf, T.; Kokorin, I., *The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them*, Singapore Journal of Legal Studies, No. 2, 2020, pp. 526-563
21. Hubbell, Z., *The Uniform Regulation of Virtual-Currency Business Act: Advancing State Regulatory Interests in a Truly Cashless Economy*, Jurimetrics, Vol. 59, No. 3, 2019, pp. 313-339
22. Hughes, S. J., Property, Agency, and the Blockchain: New Technology and Longstanding Legal Paradigms, Wayne Law Review, Vol. 65, 2019, pp. 57-80
23. Kleiner, C., *Cryptocurrencies as Transnational Currencies?*, in: Benicke C; Huber S. (eds.), National, International, Transnational: Harmonischer Dreiklang im Recht. Festschrift für Herbert Kronke zum 70. Geburtstag, Bielefeld, 2020, pp. 979-988
24. Lehmann, M., *National Blockchain Laws as a Threat to Capital Markets Integration*, Uniform Law Review, Vol. 26, No. 1, 2021, pp. 148-179

25. Lehmann, M., *Who Owns Bitcoin? Private Law Facing the Blockchain*, Minnesota Journal of Law, Science & Technology, Vol. 21, No. 1, 2019, pp. 93-136
26. Low, K. F. K., *Bitcoins as Property: Welcome Clarity?*, Law Quarterly Review, Vol. 136, No. 3, 2020, pp. 345-349
27. Ng, M.*, Choice of law for property issues regarding Bitcoin under English law*, Journal of Private International Law, Vol. 15, No. 1, 2019, pp. 315-338
28. Ooi, M., *Choice of Law in the Shifting Sands of Securities Trading*, in: Dickinson A.; Peel, E. (eds.), A Conflict of Laws Companion. Essays in Honour of Adrian Briggs, Oxford, 2021, pp. 199-224
29. Paech, P., *Conflict of Laws and Relational Rights*, in: Gullifer L.; Payne, J. (eds), Intermediation and Beyond, Oxford, 2019, pp. 289-308
30. Solinas, M., *Investors' Rights in (Crypto) Custodial Holdings: Ruscoe v Cryptopia Ltd (in Liquidation*), Modern Law Review, Vol 84 No.1, 2021, pp. 155-167
31. Steinrötter, B., *International Jurisdiction and Applicable Law*, in: Maume, P.; Maute, L.; Fromberger, M. (eds.), The Law of Crypto Assets. A Handbook, München, Oxford and Baden-Baden, 2022, pp. 69-108
32. Vadalà, R. M., *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, Giurisprudenza italiana, 2021, pp. 2225-2231
33. Werbach K.; Cornell, N., *Contracts Ex Machina*, Duke Law Journal, Vol. 67, No. 2, 2017, pp. 313-382

EU LAW

1. Council of the European Union, Letter to the Chair of the European Parliament Committee on Economic and Monetary Affairs, doc. 13198/22 of 5 October 2022
2. Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims - General approach (9050/21), 28 May 2021
3. Directive 2002/47/EC of the European Parliament and of the Council on financial collateral arrangements [2002] OJ L168/43
4. Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L41/73, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 [2018] OJ L156/43
5. Directive (EU) 2019/2177 of the European Parliament and of the Council [2019] OJ L334/155
6. European Parliament Economic and Social Committee, *Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937*, (A9-0052/2022 pf 17 March 2022)
7. European Parliament resolution on virtual currencies [2016] OJ/C 76

8. European Parliament resolution with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets [2020] (2020/2034(INL)), P9_TA(2020)0265
9. Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) [2021] COM/2021/422 final
10. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [2020] COM/2020/593 final
11. Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims [2018] COM(2018) 96 final
12. Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150

HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW

1. Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, 5 July 2006

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Decreto legislativo No. 125 of 4 October 2019, Gazz. Uff., No. 252 of 26 October 2019
2. Decreto legislativo No. 90 of 25 May 2017, Gazz. Uff., No. 140 of 19 June 2017 - Suppl. Ord. No. 28
3. Decreto legislativo No. 231 of 21 November 2007, Gazz. Uff., No. 290 of 14 December 2007 - Suppl. Ord. No. 268
4. Uniform Law Commission, Uniform Regulation of Virtual-Currency Businesses Act (URVCBA)
5. Uniform Law Commission, Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act (USCL for URVCBA)
6. Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 25. September 2020, RO 2021 33
7. Verordnung zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 18. Juni 2021, RO 2021 400
8. Messaggio concernente la legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito del 27 novembre 2019, FF 2020 223, 232
9. Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987, SR 291
10. Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220 (Swiss Civil Code of Obligations)
11. Gesetz über elektronische Wertpapiere (eWpG) vom 3. Juni 2021 (*BGBl.* I S. 1423)
12. *Osbourne v Persons Unknown Category A & Ors* [2023] EWHC 39 (KB)
13. *LMN v Bitflyer Holdings Inc & Ors* [2022] EWHC 2954 (Comm)

14. *D'Aloia v Person Unknown & Ors* [2022] EWHC 1723 (Ch)
15. *Tulip Trading Ltd v Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch)
16. *Osbourne v Persons Unknown & Anor* [2022] EWHC 1021 (Comm)
17. *Fetch.AI Lrd & Anor v Persons Unknown Category A & Ors* [2021] EWHC 2254 (Comm)
18. *Wright v McCormack* [2021] EWHC 2671 (QB)
19. *Wright v Ver* [2020] EWCA Civ 672
20. *Ion Science & Duncan Johns v Persons Unknown* (unreported) (21 December 2020)
21. *Liam David Robertson v Persons Unknown* (unreported), quoted in *AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm)
22. *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03
23. *Vorotyntseva v MONEY-4 Ltd (t/a nebeus.com) & Ors* [2018] EWHC 2596 (Ch)
24. *National Provincial Bank v Ainsworth* [1965] UKHL
25. Cassazione Penale (Sez. II), 30 November 2021, No. 44337 (unpublished).
26. Cassazione Penale (Sez. II), 17 September 2020, No. 26807, Giurisprudenza italiana, 2021, pp. 2224-2225
27. Tribunale di Firenze (Sez. fall.), 21 January 2019, No. 18, Giurisprudenza italiana, 2020, pp. 2657-2659
28. Tribunale di Firenze, 19 December 2018, No. 6, I Contratti, 2019, pp. 661-669

WEBSITE REFERENCES

1. Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments, *The use of DLT in post-trade processes*, ECB, 2021, [https://www.ecb.europa.eu/pub/pdf/other/ecb.20210412_useofdltposttradeprocesses~958e3af1c8.en.pdf?2779d0668b55434a0e67174b3f1183a4], Accessed 28 February 2023
2. Asamblea Legislativa, *El Salvador, the first country in the world to recognize Bitcoin as legal tender*, 2021, [https://www.asamblea.gob.sv/node/11282], Accessed 28 February 2023
3. Bank for International Settlements, *Annual Economic Report*, 2018, [https://www.bis.org/publ/arpdf/ar2018e.htm], Accessed 28 February 2023
4. Bank for International Settlements, Committee on Payments and Market Infrastructures, *Digital Currencies*, 2015, [https://www.bis.org/cpmi/publ/d137.htm], Accessed 28 February 2023
5. CoinMarketCap, *Today's Cyptocurrency Prices by Market Cap*, [https://coinmarketcap.com/], Accessed 28 February 2023
6. Committee on Payments and Market Infrastructures, *Distributed ledger technology in payment, clearing and settlement: An analytical framework*, BIS, 2017, [https://www.bis.org/cpmi/publ/d157.pdf], Accessed 28 February 2023
7. Conlon, T., Corbet, S., Hu, Y., *The Collapse of FTX: The End of Cryptocurrency's Age of Innocence*, SSRN 2022, [https://ssrn.com/abstract=4283333 or http://dx.doi.org/10.2139/ssrn.4283333], Accessed 28 February 2023

8. Diem Association, *Welcome to the Diem project*, [https://www.diem.com/en-us/], Accessed 28 February 2023
9. ECB Crypto-Assets Task Force, *Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area* (Occasional Paper Series No. 247), 2020, [https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf], Accessed 28 February 2023
10. European Law Institute, *ELI Principles on the use of Digital Assets a s a Security*, [https://www.europeanlawinstitute.eu/projects-publications/completed-projects/use-of-digital-assets-as-security/], Accessed 28 February 2023
11. European Banking Authority (EBA), *EBA Opinion on 'Virtual Currencies'*, 2014, [https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1], Accessed 28 February 2023
12. European Central Bank, *Virtual Currency Schemes*, 2012, [https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf], Accessed 28 February 2023
13. European Central Bank (ECB), *Virtual currency schemes – a further analysis*, 2015, [https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf], Accessed 28 February 2023
14. European Securities and Markets Authority (ESMA), *Advice: Initial Coin Offerings and Crypto-Assets*, 2019, [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf], Accessed 28 February 2023
15. European Securities and Markets Authority (ESMA), *European Banking Authority (EBA), and European Insurance and Occupational Pensions Authority (EIOPA), ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*, 2018, [https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf], Accessed 28 February 2023
16. Evans, J. B.; Scheibe, A. C., *A Flurry of CFTC Actions Shock the Cryptocurrency Industry*, McDermott, 2021, [https://www.mwe.com/it/insights/a-flurry-of-cftc-actions-shock-the-cryptocurrency-industry/], Accessed 28 February 2023
17. Financial Conduct Authority (FCA), *Guidance on Crypto-assets (Consultation Paper CP19/3)*, 2019, [https://www.fca.org.uk/publication/consultation/cp19-03.pdf], Accessed 28 February 2023
18. Financial Markets Law Committee, *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*, 2018, [http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf], Accessed 28 February 2023
19. Financial Markets Law Committee, *Issues of Legal Uncertainty Arising in the Context of Virtual Currencies*, 2016, [http://fmlc.org/wp-content/uploads/2018/03/virtual_currencies_paper_-_edited_january_2017.pdf], Accessed 28 February 2023
20. German Federal Financial Supervisory Authority ("BaFin"), *Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG)*, 2020, [https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html?nn=9451720#O4], Accessed 28 February 2023

21. German Federal Financial Supervisory Authority ("BaFin"), *Virtual Currency (VC)*, 2017, [https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html], Accessed 28 February 2023
22. He, D. *et al*, *Virtual Currencies and Beyond: Initial Considerations (IMF Staff Discussion Note)*, International Monetary Fund, 2016, [https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf], Accessed 28 February 2023
23. HM Treasury, *Consultation and call for evidence on "Future financial services regulatory regime for cryptoassets"*, 2023, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf], Accessed 28 February 2023
24. Houben R.; Snyers, A., *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, 2018, [https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf], Accessed 28 February 2023
25. International Monetary Fund, *Staff Concluding Statement of the 2021 Article IV Mission*, 2021, [https://www.imf.org/en/News/Articles/2021/11/22/mcs-el-salvador-staff-concluding-statement-of-the-2021-article-iv-mission], Accessed 28 February 2023
26. ISDA; McCann FitsGerald; r3, *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Irish Law*, 2020, [https://www.isda.org/a/ACrTE/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-Irish-Law.pdf], Accessed 28 February 2023
27. ISDA, Jones Day; and r3 *"Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: French Law",* 2020, [https://www.isda.org/a/ZCrTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT-French-Law.pdf], Accessed 28 February 2023
28. Karim, M.; Tomova, G., *Research Note: Cryptoasset consumer research 2021*, Financial Conduct Authority, 2021, [https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021], Accessed 28 February 2023
29. Law Commission, *"Digital assets: Consultation paper"*, No 256 of 28 June 2022, [https://www.lawcom.gov.uk/document/digital-assets-consultation-paper/], Accessed 28 February 2023
30. Law Commission, *Digital Assets Interim Update*, 24 November 2021, [https://www.lawcom.gov.uk/project/digital-assets/], Accessed 28 February 2023
31. Law Commission, *"Digital assets: Final report"*, No 412 of 23 June 2023, [https://www.lawcom.gov.uk/document/digital-assets-final-report-2/], Accessed 20 July 2023
32. Libra Association Members, *White Paper – An Introduction to Libra*, [https://sls.gmu.edu/pfrt/wp-content/uploads/sites/54/2020/02/LibraWhitePaper_en_US-Rev0723.pdf], Accessed 28 February 2023
33. Moir, A. *et al*, *High Court considers where cryptocurrencies are located and compels disclosure of information by cryptocurrency exchanges outside the UK*, Herbert Smith Freehills, 2021, [https://hsfnotes.com/litigation/2021/02/24/high-court-considers-where-cryptocurrencies-are-located-and-compels-disclosure-of-information-by-cryptocurrency-exchanges-outside-the-uk/], Accessed 28 February 2023

34. Nabilou, H., *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, SSRN, 2022, [http://dx.doi.org/10.2139/ssrn.4022676], Accessed 28 February 2023
35. Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin, 2009, [https://bitcoin.org/bitcoin.pdf], Accessed 28 February 2023
36. R.I. Gen. Laws § 6-56-1-6-56-11 (Current through Chapter 429 (all legislation) of the 2021 Session, including all corrections and changes made by the Director of Law Revision), [https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DF-62M1-DYB7-W0YY-00000-00&context=1516831], Accessed 28 February 2023
37. Sleave, L., *Cryptocurrency Fraud - The High Court Considers The Position Of 'Crypto-assets'*, Mondaq Business Briefing, 2021, [https://link.gale.com/apps/doc/A663644295/ITOF?u=milano&sid=bookmark-ITOF&xid=03ffe69d], Accessed 28 February 2023
38. Swiss Federal Council report, *Legal framework for distributed ledger technology and blockchain in Switzerland. An overview with a focus on the financial sector*, 2018, [https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf], Accessed 28 February 2023
39. Takahashi, K., *Blockchain-based Negotiable Instruments (with Particular Reference to Bills of Lading and Investment Securities)*, SSRN, 2021, [https://ssrn.com/abstract=3937664], Accessed 28 February 2023
40. The Law Society, [https://www.lawsociety.org.uk/campaigns/lawtech/guides/lawtech-delivery-panel], Accessed 28 February 2023
41. UK Jurisdiction Taskforce, *Legal statement on crypto-assets and smart contracts*, Tech Nation, 2019, [https://technation.io/about-us/lawtech-panel], Accessed 28 February 2023
42. UNIDROIT, *Draft UNIDROIT Principles on Digital Assets and Private Law*, UNIDROIT 2023 Study LXXXII-PC, 2023, [https://www.unidroit.org/wp-content/uploads/2023/01/Draft-Principles-and-Commentary-Public-Consultation.pdf], Accessed 28 February 2023
43. UNIDROIT, *Principles on Digital Assets and Private Law*, as approved by the Governing Council at its 102th session, Rome, 10-12 May 2023, C.D, (102), 2023, [https://www.unidroit.org/wp-content/uploads/2023/04/C.D.-102-6-Principles-on-Digital-Assets-and-Private-Law.pdf], Accessed 19 July 2023
44. Uniform Law Commission, [https://www.uniformlaws.org/viewdocument/final-act-154?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778&tab=librarydocuments], Accessed 28 February 2023
45. Uniform Commercial Code Amendments, 2022, [https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac#:~:text=The%202022%20amendments%20to%20the,intelligence%2C%20and%20other%20technological%20developments], Accessed 28 February 2023
46. U.S. President Executive Order on Ensuring Responsible Development of Digital Assets of 9 March 2022, [https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/], Accessed 28 February 2023
47. US Securities and Exchange Commission, *Funds Trading in Bitcoin Futures – Investor Bulletin*, 2021, [https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/funds], Accessed 28 February 2023

48. World Bank Group (Harish Natarajan, Solvej Krause, and Harish Gradstein), *Distributed Ledger Technology (DLT) and blockchain*, FinTech Note No. 1, 2017, [http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf], Accessed 28 February 2023
49. Wright A.; De Filippi, P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*,, SSRN, 2015, [https://papers.ssrn.com/abstract=2580664], Accessed 28 February 2023
50. Wyo. Stat. § 34-29-102 (Current through 2021 General Session and Special Session of the Wyoming Legislature, Subject to revisions by LSO, [https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DC-SNC3-CH1B-T54F-00000-00&context=1516831], Accessed 28 February 2023
51. Zetzsche, D. A. *et al*, *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*, EBI Working Paper Series No. 2020/77, SSRN, 2020, [http://dx.doi.org/10.2139/ssrn.3725395], Accessed 28 February 2023

UDK 004.056.53:342.7]:341.645(4-67EU)
Original scientific paper

DATA PROTECTION AND CYBERSECURITY: CASE-LAW OF TWO EUROPEAN COURTS*

Dunja Duić, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
dduic@pravos.hr

Tunjica Petrašević, PhD, Full Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
tpetrase@pravos.hr

ABSTRACT

Cybersecurity is not easily defined. The 2019 EU Cybersecurity Act defines it as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[1] Enduringly, cybersecurity was associated with national security, without consideration of what 'secure' Internet means for individual users. In reality, cybersecurity policy focused by and large on systems rather than users, i.e., people. However, as a policy area concerned with online behavior regulation, its definition and implementation inevitably has profound implications for human rights, especially in regard to data protection and freedom of expression. Unsurprisingly, cybersecurity has become a new human rights battleground.[2] The EU Cybersecurity Act and subsequent legislation represent a normative shift in our conception of data ownership, putting ownership and control of personal information in the hands of the user rather than the service provider. Luckily, there have been positive legislative shifts regarding data protection in the context of the EU cybersecurity policy at EU

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1 Art. 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151, pp. 15–69.

2 More at: Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights,* OpenDemocracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights/], Accessed 25 November 2022.

level. But are they (or will they be) adopted by European courts? To answer, this paper peers into the relevant case-law of the Court of Justice of the EU as well as of the European Court of Human Rights.

***Keywords**: data protection, cybersecurity, human rights, European Union, Council of Europe, Court of Justice of the EU, European Court of Human Rights*

1. INTRODUCTION

In these times of globalization and all-digitalization, technological advancements are a double-edged sword to human rights and freedoms. The advent of the Internet and its pervasiveness stand as one of key such developments of the past 30 years. The Internet has come to pervade the entire social fabric, from communication and learning, to work and shopping.[3] But with the benefits of digitalization come also new threats.[4] As part and parcel of technological advancements, cybersecurity has become integral to a number of countries' and the EU's political action. Until recently, as part of national policy, cyberspace was tied to digital market, cybersecurity, migration and/or terrorism issues. Over time, due to its importance and security issues, the EU included cyberspace and cybersecurity into the scope of the Common Foreign and Security Policy (CFSP).[5]

For clarity, the paper will first turn to defining data protection and cybersecurity and, next, to explaining their interrelatedness.

Essential in the domain of personal data protection in the EU is the General Data Protection Regulation (GDPR), under which personal data is *any information relating to identified or identifiable natural persons, whereby an identifiable natural person is one who can be identified by a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.[6]

There are a number of ways of defining cybersecurity. Microsoft defines it as *the practice of protecting one's digital information, devices, and assets (digital security),*

---

3 Wiśniewski, A., *The European Court of Human Rights and Internet-Related Cases,* Bialystok Legal Studies, Vol. 26, No. 3, 2021, p. 110.

4 Schünemann, W. J.; Baumann, M-O. (eds.), *Privacy, Data Protection and Cybersecurity in Europe*, Springer, Cham, 2017, pp. 1-2.

5 Duić, D., *The EEAS as a Navigator of EU Defence Aspects in Cyberspace*, European Foreign Affairs Review, Vol. 26, No. 1, 2021, pp. 101-114.

6 Art. 4 of 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), [2016] OJ L 119, pp. 1–88.

which includes one's personal information, accounts, files, photos, and even money.[7] Per the 2019 EU Cybersecurity Act, *cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*[8] *The* Freedom Online Coalition (FOC) sees it as[9] *the preservation – through law, policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.*[10]

Internet should be 'free' but also secure. For a long time, cybersecurity was strongly tied to national security, disregarding what 'secure' Internet means for individual users.[11] As a result, cybersecurity policy was angled at systems more than people. However, as a policy area concerned with online behavior regulation, its definition and implementation has profound implications for human rights, especially in regard to data protection and freedom of expression. It is then hardly surprising that – to quote the OpenDemocracy forum – cybersecurity has become a new human rights battleground.[12]

In support of their position, OpenDemocracy underline several important facts. First, that cybersecurity policy was framed exclusively by national security agencies and select private sector interests (e.g. telecommunications operators). Second, that government services, which store a wide range of sensitive data (from taxation to health records), are rapidly migrating online, while (as third) the monopoly-holding tech companies elite's business model relies on the processing, storage, and monetization of the people's personal information. Correspondingly, cybersecurity has become fused with 'national security', leaving by the wayside the

---

7 *What is cybersecurity?*, [https://support.microsoft.com/en-us/topic/what-is-cybersecurity-8b6efd59-41ff-4743-87c8-0850a352a390], Accessed 25 November 2022.

8 Art. 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151, pp. 15–69.

9 The Freedom Online Coalition (FOC) is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide. See more at: Freedom Online Coalition, *Aims and Priorities*, [https://freedomonlinecoalition.com/aims-and-priorities/], Accessed 25 November 2022.

10 See: Freedom Online Coalition, *Why Do We Need a New Definition for Cybersecurity?,* [https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity], Accessed 25 November 2022.

11 Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights*, Open Democracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights], Accessed 25 November 2022.

12 The statement was taken from the OpenDemocracy forum as an independent international media platform. See more: Puddephatt; Kaspar, *op. cit.*, note 2.

interests of individual users and what 'secure' Internet might mean for them. Such understanding of cybersecurity – in which surveillance powers run wild, 'backdoors' undermine encryption and anonymity, and accountability is an anomaly – may easily come to diametrically oppose individual security and individual (human) rights.[13] Per Pavlova, countries should find the right balance between fundamental rights and freedoms of their citizens, with the aim of achieving an appropriate level of national security that ensures respect for fundamental rights. Countries should not be able to hide their failure to do so behind the pretext of human rights vs. national security.[14]

Cybersecurity must begin to be understood as a policy centered on the security and rights of the end user rather than systems, as provided for under the 2019 EU Cybersecurity Act. Would that imply a normative shift in our understanding of data ownership, putting the reins of ownership and control of personal data in the hands of the user instead of the service provider? A democratic society provides cybersecurity that entails the informed consent of the population – in other words, it ensures that parties other than security agencies have a say in the conversation around it that will ultimately result in cybersecurity being understood above all as the protection of persons.[15] Luckily, there have been positive legislative shifts regarding data protection in the context of the EU cybersecurity policy at EU level (to be discussed below). But are they (or will they be) adopted by European courts? To answer this, this paper peers into the relevant case-law of the Court of Justice of the EU (CJEU) as well as of the European Court of Human Rights (ECtHR).

This paper updates the present authors' previous research in data protection in the CJEU and ECtHR case-law given new developments in the area.[16]

---

13 *Ibid*.

14 Pavlova, P., *Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups*, Peace Human Rights Governance, Vol. 4, No. 3, 2020, p. 409.

15 See: Puddephatt, A.; Kaspar, *op. cit.*, note 2; Duić, D., *Common Security and Defence Policy and Cyber Defence*, in: Brill, A.; Misheva, K.; Hadji-Janev, M. (eds.), *Toward Effective Cyber Defense in Accordance with the Rules of Law*, IOS Press, Amsterdam, 2020, pp. 32-42.

16 Petrašević, T.; Duić, D., *Standards of Human Rights Protection in the Domain of Personal Data Protection: Strasbourg vs Luxemburg*, in: Sander, G. G.; Poščić, A; Martinović, A. (eds.), Exploring the Social Dimension of Europe- Essays in Honour of Nada Bodiroga-Vukobrat, Verlag Dr. Kovač, Hamburg, 2021, pp. 215-231.

2. A BRIEF EVOLUTION OF INTERNATIONAL AND EU CYBERSECURITY POLICY

In 'The right to privacy in the digital age',[17] the UN General Assembly, concerned over the negative impact of communications surveillance and interception on human rights, called on all member states to review their legislation, procedures and practice of surveillance of communications, their interception and collection of personal data and ensure full and effective implementation of their obligations in accordance with international human rights standards.[18] In its resolution on the promotion and protection of human rights on the Internet, the UN's Human Rights Council affirmed that the same rights that people have offline must also be protected online, in particular, freedom of expression.[19,20]

The European Convention on Human Rights (Convention) – a vital instrument of the Council of Europe – was adopted in 1950, at a time when the Internet was an unknown to the wider society and its creators could not have foreseen technology's current magnitude. The ECtHR must therefore interpret the Convention as a "living instrument" [21] in light of changes in the social circumstances.[22] The right to personal data protection is not an autonomous right guaranteed by the Convention. Nevertheless, the ECtHR subsumes and protects it primarily under Article 8 of the Convention – the right to private and family life, even though it can also be considered under other articles of the Convention and certain protocols.[23,24] Cybersecurity is also not regulated by the Convention or its protocols, but the ECtHR interprets the Convention considering changes in the social circumstances, taking into account technological progress, and especially the increasingly widespread use of the Internet (to be discussed in more detail below).

---

17 Resolution A/RES/68/167 adopted by the UN General Assembly on 18 December 2013 on the right to privacy in the digital age.

18 United Nations, *General Assembly backs right to privacy in digital age,* [https://news.un.org/en/story/2013/12/458232], Accessed 30 December 2022.

19 United Nations, High Commissioner for Human Rights, Resolution A/HRC/RES/32/13 on the promotion, protection and enjoyment of human rights on the Internet. See also: United Nations, High Commissioner for Human Rights, *The right to privacy in the digital age*, [https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age], Accessed 30 December 2022. See also: Pavlova, *op. cit.*, note 14, p. 398.

20 For more on development of cybersecurity policy at the international level, see: Pavlova, *op. cit.*, note 14, pp. 398-401.

21 *Demir and Baykara v Turkey*, Application No. 34503/97, Judgment, 12 November 2008, par. 146.

22 Wiśniewski, *op.cit.,* note 3, p. 110.

23 See: *Guide to the Case-Law of the European Court of Human Rights: Data protection*, Council of Europe / European Court of Human Rights, 2022 (Updated on 31 August 2022), p. 7.

24 Petrašević; Duić, *op.cit.*, note 16, pp. 223-224.

Apart from the Convention, two other important documents have been adopted under the auspices of the Council of Europe: the Convention on Cybercrime[25] (the Budapest Convention), along with its Protocol on Xenophobia and Racism Committed through Computer Systems, [26] and the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[27]

The EU is spearheading in the category of cybersecurity reinforcement, well aware that – while creating a profusion of new opportunities for the economy and society – the digital era also introduces new challenges. Cyber-incidents and cyber-attacks often bring billions of euros in losses annually. Cybersecurity, trust, and privacy form the backbone of a prosperous European Digital Single Market (EDSM). To shield the EDSM and protect infrastructure, governments, businesses and citizens, the EU has adopted a wide range of measures.[28] But how did it all begin?

In 2013, the EU adopted its first Cybersecurity Strategy on an Open, Safe and Secure Cyberspace, aimed at safeguarding an open and free cyberspace under the same EU norms, principles and values upheld 'offline'.[29] The Directive on Security of Network and Information Systems (NIS Directive), enacted in 2016, was the first tangible piece of EU law aimed at boosting the cybersecurity at EU level overall.[30] The EU Cybersecurity Act of 2019 established an EU framework for cybersecurity certification to enhance cybersecurity of digital products and services in Europe,[31] while strengthening the action of the European Union Agency for Cybersecurity (ENISA). Founded in 2004, ENISA contributes to the EU's cyber policy, improves ICT product, service and procedure reliability through a cybersecurity certification program, cooperates with member states and EU bodies, and

---

25 Convention on Cybercrime (ETS No. 185) [2001].

26 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) [2003].

27 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [1981].

28 European Commission, *Building strong cybersecurity – Brochure*, 2019, [https://digital-strategy.ec.europa.eu/en/node/1500/printable/pdf], Accessed 5 January 2023.

29 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, [2013] JOIN(2013) 1 final, par. 1.1.

30 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194, p. 1–30. In December 2020, the European Commission proposed a revision of Directive (EU) 2016/1148 (NIS2).

31 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (PE/86/2018/REV/1) [2019] OJ L 151, p. 15–69.

helps Europe prepare for future cyber challenges.[32] In 2020, the European Commission adopted the new EU Cybersecurity Strategy for the Digital Decade.[33] To increase the Internet networks and information systems security, in 2021, the Council of the EU adopted the Regulation establishing the European Cybersecurity Competence Centre (ECCC) (based in Bucharest) to aggregate investment in research, technology and industrial development in cybersecurity.[34] In May 2022, the Council extended until May 2025 the framework for restrictive measures against cyberattacks threatening the EU and its member states. The framework[35] was originally established in May 2019 as the EU's joint diplomatic response to malicious cyber activities ('cyber diplomacy toolbox'). The framework enables the EU and member states to apply all CFSP measures, including restrictive measures, where necessary, with the aim of preventing and containing malicious cyber activity aimed at undermining the integrity and security of the EU and its member states, as well as deterring from them and responding to them.[36] Cyberspace has become a matter of geopolitical competition, so the EU must be ready to respond quickly and forcefully to cyberattacks. Guidelines for strengthening the EU's position in the field of cybersecurity are provided in the Strategic Compass – the EU's action plan for strengthening the security and defense policy until 2030.[37,38]

3. RELATION OF THE TWO EUROPEAN COURTS REGARDING HUMAN RIGHTS PROTECTION

To better understand the case-law of the two European courts (the CJEU and the ECtHR) in regard to personal data protection in the context of cybersecurity, their relation in the field of human rights protection must be understood in general. Particularly interesting in that regard is that relation before and after the entry

---

32 ENISA - European Union Agency for Cybersecurity, *About*, [https://www.enisa.europa.eu/about-enisa/about/], Accessed 5 January 2023.

33 Joint communication to the European parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN/2020/18 final.

34 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT [2021] OJ L 202.

35 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L 129I.

36 Council of the EU, *Cyber-attacks: Council extends sanctions regime until 18 May 2025*, 2022, [https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025], Accessed 5 January 2023.

37 A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security [2022] 7371/22.

38 For more on the development of EU cyber policy, see: Christou, G., *Cybersecurity in the European Union*, Palgrave Macmillan, London, 2016, pp. 87-118.

into force of the Charter of Fundamental Rights of the EU[39] (Charter) that was a turning point in the development of human rights in the EU.[40]

Given that the EU (that is, the European Community as its precursor) was founded primarily for the purpose of economic integration, human rights were reasonably not in its primary focus. Human rights protection was instead entrusted to the Council of Europe as a separate international organization, of which EU member states automatically became members, as well as signatories to the Convention.[41] Below is a brief overview of the two courts' relation, including references to relevant literature, given that the topic was discussed as part of the present authors' previous research.

After being shunned, then accepted by the CJEU only as unwritten rules (general principles of law), and eventually codified in the EU Charter on Fundamental Rights, the protection of fundamental human rights in the EU came into its own only with the EU's accession to the Convention.[42] Even though after the entry into force of the Treaty of Lisbon (2009) there were no formal legal prerequisites for the EU's accession to the Convention, the CJEU still issued the highly criticized negative opinion no. 2/13 of 18 December 2014.[43,44] The consensus in literature

---

39 Charter of Fundamental Rights of the European Union [2012] OJ C 326, pp. 391–407.

40 See: Cherubini, F., *The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View of the Accession*, German Law Journal, Vol. 16, No. 6, 2015, pp. 1375-1386.

41 Petrašević, T.; Duić, D., *Opinion 2/13 on the EU accession to the ECHR*, in: Vinković, M. (ed.), New Developments in the EU Labour, Equality and Human Rights Law, J. J. Strossmayer University of Osijek – Faculty of Law, Osijek, 2015, p. 253. Petrašević, T.; Kovačić Markić, L., *Položaj nacionalnih ustavnih sudova u primjeni mehanizma prethodnog postupka s posebnim osvrtom na Ustavni sud Republike Hrvatske*, in: Bačić, A. (ed.), Pravo i politika EU: stara pitanja, novi odgovori, HAZU, Zagreb, 2020, pp. 144-145.

42 Petrašević; Markić Kovačić, *op. cit.*, note 41, pp. 145-146. Petrašević; Duić, *op. cit.*, note 16, pp. 251-267. Petrašević, T., *The relation of Human Rights and market freedoms in case law of the CJEU*, in: Primorac, Ž.; Bussoli, C.; Recker, N. (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, Varaždin/Split, 2016, pp. 142-145.

43 E.g. Lazowski, A.; Wessel, R.A., *When Caveats Turn into Locks: Opinion 2/13 on Accession of the European Union to the ECHR*, German Law Journal, Vol. 16, No. 1, 2015, pp. 179 – 212. See blog discussions: Peers, S., *The CJEU and the EU's Accession to the ECHR: A Clear and Present Danger to Human Rights Protection*, EU L. ANALYSIS BLOG, 2014, [http://eulawanalysis.blogspot.com.es/2014/12/the-cjeu-and-eus-accession-to-echr.html], Accessed 30 December 2022. Douglas-Scott, S., *Opinion 2/13 on EU Accession to the ECHR: A Christmas Bombshell from the European Court of Justice*, U.K. CONST. L. BLOG, [http://ukconstitutionallaw.org], Accessed 30 December 2022. Gotev, G., *Court of Justice rejects draft agreement of EU accession to ECHR*, Euractiv, 2014, [http://www.euractiv.com/sections/eu-priorities-2020/court-justice-rejects-draft-agreement-eu-accession-echr-310983], Accessed 30 December 2022.

44 For more on Opinion 2/13 on the EU accession to the ECHR, see: Petrašević; Duić, *op. cit.*, note 16, pp. 251-266.

on the exhaustively discussed topic[45] of the formal grounds of said CJEU's opinion is that behind it likely lay a power struggle between the CJEU and the ECtHR. [46] Namely, in case of accession, the decisions of the CJEU in the field of human rights protection would fall under the supervision of the ECtHR. Consequently, the ECtHR would *de facto* become superior to the CJEU.

Namely, even though the Convention is still not formally part of the EU legal order, by virtue of the provision of Art. 52(3) of the EU Charter of Fundamental Rights, the standards set by the ECtHR are binding on the CJEU. Specifically, to the extent to which the EU Charter contains rights corresponding to those guaranteed by the ECHR, the meaning and scope of application of those rights are equal to those of the Convention. Apart from the obligation to consider relevant issues, i.e., to avoid contradictions in relation to the ECtHR's case-law on relevant issues, this also includes the implementation of its awards, with a view to achieving a uniform interpretation of fundamental and human rights. The CJEU's consistency in this regard after entry into force of the Treaty of Lisbon, i.e., of the EU Charter, evidences itself best from its judgements.[47]

In the field of human rights protection today, the two courts increasingly frequently take opposing positions on the protection of the same fundamental human right or freedom guaranteed both by the Convention and the Charter. National, and particularly constitutional courts are often faced with the dilemma of whether to prioritize the views of the Strasbourg or Luxembourg court.[48]

Having come a long way, human rights protection in the EU today occupies a central place and stands as a primary EU right. Nevertheless, while the ECtHR is exclusively tasked with the protection of fundamental human rights and freedoms, the CJEU – in addition to protecting human rights – is tasked with preserving the goals of the EU, particularly the functioning of the EU common market, which requires a delicate balancing of different interests.[49]

In sum, the CJEU does protect human rights, but in light of EU goals, as evident from its case-law. To remain within the scope of this paper, the relation of the ECtHR and the CJEU will be observed exclusively through the lens of data pro-

---

45 Petrašević, T.; Poretti, P., *Pravo na suđenje u razumnom roku – postoji li (nova) praksa Suda Europske unije?*, Harmonius - Journal of Legal and Social Studies in South East Europe, Vol. 7, No. 1, 2018, p. 189.

46 Petrašević; Markić Kovačić, *op.cit.*, note 41, p. 146.

47 Petrašević; Poretti, *op.cit.*, note 45, p. 193.

48 *Ibid.*

49 See: Jakir, V., *Human Rights – With or without the internal market*, Zagreb, 2012, master thesis.

tection in the context of cybersecurity, and in that adding to the present authors' previous research in that area.[50]

4. CASE-LAW OF THE TWO EUROPEAN COURTS ON DATA PROTECTION IN THE CONTEXT OF CYBERSECURITY

The global war on terrorism has brought to the forefront national and public security and led to security services' mass-invasion of personal data privacy. It is upon the CJEU and the ECtHR to assess the merits of such invasions through testing their necessity and proportionality and evaluating their compliance with legitimate objectives.[51] The standards set by the ECtHR were largely complied with by the CJEU in its rulings, including the ECtHR's test of necessity and proportionality. The CJEU was faced mainly with issues of blanket coverage that enabled mass surveillance and access to user data under EU Directives to national security services. The CJEU declared such measures invalid on grounds of failing the necessity and proportionality test due to the lack of legal measures that could protect those were not suspects under law (more on this below, on *Schrems*).[52]

Both courts acknowledge through their case-law the society's need to fight serious crime and terrorism. While such measures may be indispensable to tackle security challenges such as fighting terrorism and preventing serious transnational crimes, they must not go beyond the strictly necessary. The two courts have also highlighted the importance of the existence of legal remedies against such measures.[53]

The two European courts are tasked with the protection of citizens from the state machinery and security agencies. To do so, they are to carry out the necessity and proportionality tests[54] while finding equilibrium between the right of individuals to data privacy and the national security of member states. The balancing act is made only more arduous by the ongoing global anti-terrorism war.[55]

In contrast to the Convention, the Charter in its Article 8 recognizes the protection of personal data as an independent right. Nevertheless, the ECtHR protects

---

50 Petrašević; Duić, *op.cit.*, note 16, pp. 215-231.

51 Syed, H., *Data Protection Rights & National Security Objectives: Critical Analysis of ECtHR and CJEU Case Law*, Nor. Am. Aca. Res., Vol. 2, No. 3, 2019, p. 155.

52 *Ibid.*

53 *Ibid.*

54 See more on the proportionality and necessity tests: Omejec, J., *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava*, Novi informator, Zagreb, 2013, pp. 1253-1267.

55 Syed, *op.cit.*, note 51, p. 157.

that right under Art. 8 of the Convention (the right to privacy). The term 'personal data' itself has a similar meaning in the two courts' practice.[56]

Below, an analysis of selected ECtHR and CJEU case-law with introductory remarks specific to each court. The concluding remarks offer a comparison of the two courts' positions.

4.1. Case-law of the ECtHR

There is a modest number of Internet-related cases in the ECtHR case-law: to classify as such, a case must contain a cross-border element. In online communication, data are usually transmitted via servers located in different territorial jurisdictions. Occasionally, the establishing of the state of jurisdiction causes significant difficulties.[57] Narrowed to cases concerning data protection in the context of cybersecurity only, the number dwindles even further. A search of the ECtHR case-law (via the HUDOC database) by the terms 'data protection' and 'cybersecurity returns only one result: *K.U. v Finland.*[58] Replacing 'cybersecurity' with 'cyberspace' also returns only one case: *Big Brother Watch.*[59] Only by expanding the search through replacing 'cybersecurity' with 'national security' does it return a sizable number of cases: 1632. (Importantly, these cases include protection of privacy in general, and not only data protection, given that the search cannot be narrowed by that specific criterion/term.) Below is an analysis of selected data protection cases examined by the ECtHR through the lens of national security and with a special reference to cybersecurity.

On the one hand, in deciding certain cases, the ECtHR takes into account the Internet's advantages. In particular, the court highlights the Internet's value to the exercise of certain rights, such as the freedom of expression, observing that it has become one of the main vehicles for the exercising of the right to freedom and for receiving and sharing information and ideas.[60] The ECtHR also recognizes the Internet's value in enhancing the general news availability and facilitating information dissemination, as well as its significance in education and research, especially given its wide availability to the public and being free for use.[61]

---

56 *Ibid*., p. 159.

57 Wiśniewski, *op.cit*., note 3, p. 112.

58 *K.U. v Finland*, Application No. 2872/02, Judgment, 2 December 2008.

59 *Big Brother Watch and Others v the United Kingdom*, Application Nos. 58170/13, 62322/14, 24960/15, Judgment, 13/09/2018; and *Big Brother Watch and Others v the United Kingdom*, Application Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment, 25 May 2021.

60 *Cengiz and Others v Turkey*, Application Nos. 48226/10, 14027/112015, Judgment, 1 December 2015, par. 49.

61 Wiśniewski, *op.cit*., note 3, p. 113.

On the other hand, the ECtHR is aware of the Internet's disadvantages: the ease, extent, and speed of online data sharing, as well as the permanence of the shared data.[62] As the court sees it, compared to traditional media, this alone may significantly exacerbate the repercussions of unlawful speech on the Internet.[63]

The ECtHR is not blind to the dangers of the Internet for human rights, finding that *the rapid development of telecommunications technologies in recent decades has led to the emergence of new types of crime and has also enabled the commission of traditional crimes by means of new technologies.*[64] Clearly aware of the Internet's anonymous character, the court sees its crime-facilitating qualities.[65] Cybercrime (offences against or through computer systems) has become a substantial threat to human rights, democracy, and the rule of law, as well as international peace and stability, with enormous social and economic consequences. The Council of Europe is attempting to combat it.[66]

As its case-law shows, the ECtHR considers that personal data protection and retention falls under private life as protected by Article 8 of the Convention.[67] While the fundamental goal of Article 8 is to safeguard the individual from arbitrary government intrusion, there may be positive responsibilities inherent in effective respect for private or family life.[68] In this sense, member states have a positive obligation to preserve the privacy of individuals on the Internet.

In *K. U. v. Finland* – one of the most notable cases in that regard – the ECtHR took the view that a state may be liable in regard to third-party personal data storage providers. The case involved a provider's refusal to disclose data on the user of the IP address from which certain content defaming to the minor applicant were uploaded. The provider invoked its obligation to comply with the then applicable Finnish law in regard to the protection of the confidentiality of electronic communications. The ECtHR found that, although the exercise of the right to freedom of expression and secrecy of electronic communications is essential, electronic com-

---

62 *Delfi AS v Estonia*, Application No. 64569/09, Judgment, 16 June 2015, par. 147. More in: Wiśniewski, *op.cit.*, note 3, p. 114.

63 *Delfi AS v. Estonia*, *op. cit.*, note 62, par. 147.

64 *K.U. v Finland*, *op. cit.*, note 58, par. 22. More in: Wiśniewski, *op.cit.*, note 3, p. 114.

65 *Ibid.*

66 More at: Council of Europe, *Action against Cybercrime*, 2023, [https://www.coe.int/en/web/cybercrime], Accessed 5 January 2023.

67 See: *S. Marper v the United Kingdom*, Application Nos. 30562/04 and 30566/04, Judgment, 4 December 2008, par. 103.

68 *Airey v Ireland*, Application No. 6289/73, Judgment, 9 October 1979, par. 32.

munications and Internet services' users must be guaranteed protection of privacy and freedom of expression.[69]

Governments frequently obtain data through secret surveillance to safeguard national security. Such secret surveillance systems and actions must contain legal safeguards and be supervisable:[70] even where created to preserve national security, such systems risk the weakening or even destroying of democracy in the name of preserving it.[71] The ECtHR must therefore be convinced that appropriate and effective safeguards against abuse of such systems exist. In brief, where personal information is stored in the interests of national security, robust and effective safeguards against government misuse must be in place. Where such protections exist, the ECtHR will not necessarily find a violation of Article 8.[72]

Another notable case in the domain of mass surveillance – *Big Brother Watch and Others v. the United Kingdom*[73] – involved three applications against the United Kingdom lodged by companies, charities, organizations and individuals. The case was brought after Edward Snowden (a former associate of the US National Security Agency) exposed the surveillance and data sharing programs between the US and the UK. The applicants argued that the nature of their activities implied that their electronic communications had been intercepted or obtained by the UK's intelligence services after being intercepted by foreign governments, and/or obtained by the UK's authorities via communications service providers (CSPs).

After examining the regime for bulk interception of communications, the ECtHR found a number of system deficiencies and a violation of Articles 8 and 10 of the Convention. Since the court did not find a violation of Article 8 with regard to the intelligence sharing regime, the applicants requested a referral to the Grand Chamber. In its decision of 25 May 2021, the Grand Chamber largely confirmed the judgment of the first-instance council but made a clear distinction between targeted and mass surveillance. It also set clear mass surveillance guidelines, starting from the so-called Weber Guidelines that the ECtHR defined in *Weber*,[74] as well as eight additional guarantees (which fall outside the scope of this paper).

---

69 *K.U. v. Finland, op. cit.,* note 58, par. 43.

70 See: *Weber and Saravia v Germany*, Application No. 54934/00, Decision, 29 June 2006, par. 94. *Liberty and Others v the United Kingdom*, Application No. 58243/00, Judgment, 1 July 2008, par. 62.

71 See: *Klass and Others v Germany*, Application No. 5029/71, Judgment, 6 September 1978, paras. 49-50.

72 See also: *Youth Initiative for Human Rights v Serbia*, Application No. 48135/06, Judgment, 25 June 2013.

73 *Op. cit.*, note 59.

74 *Weber and Saravia v. Germany*, *op. cit.*, note 70.

Big Brother Watch was only the first in a slew of cases in which the ECtHR had the opportunity to examine extensive surveillance and data retention regimes of Council of Europe member states such as Sweden[75], Hungary[76], Russia[77], Germany[78], Moldova[79] and Romania.[80,81] The positions of the ECtHR in these cases can be summarized as follows:

- interference with rights under Art. 8 to the Convention is proportionate where the state has a legitimate interest, such as prevention of serious crime for a short period (3 months), and where it affects only the person of interest,[82]
- random secret surveillance by intelligence agencies with blanket access to mass data is considered a serious interference with rights under Article 8 to the Convention,[83]
- national legislation deploying advanced anti-terrorism technologies is considered a legitimate aim, but the lack of legal measures to prevent blanket data access by the security agencies is considered an interference with the rights under Article 8 to the Convention,[84]
- national court's decision permitting blanket interception of communication for a period of one and a half month is considered a violation of Article 8 (and Article 13) to the Convention.[85,86]

A more recent case, *Volodina v. Russia*,[87] concerned the state's obligation to protect the applicant from cyber violence, including the nonconsensual publication of her intimate photographs, stalking and impersonation, and the state's obligation to conduct an effective investigation into such acts. The applicant, a Russian national and resident,[88] claimed that the Russian authorities failed to protect her from repeated acts of cyber harassment. In particular, she claimed that her ex-partner

---

75 See: *Centrum för Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021.

76 *Szabó and Vissy v Hungary*, App. No. 37138/14, Judgment, 12 January 2016.

77 *Roman Zakharov v Russia*, Application No. 47143/06, Judgment, 4 December 2015.

78 *Uzun v Germany*, Application No. 35623/05, Judgment, 2 September 2010.

79 *Iordachi and Others v Moldova*, Application No. 25198/02, Judgment, 10 February 2009.

80 *Dumitru Popescu v Romania,* Application No. 71525/01 (No. 2), Judgment [2007].

81 Zalnieriute, *op. cit.,* note 75, pp. 587-588.

82 *Uzun v Germany*, *op. cit.*, note 78.

83 Zakharov, *op. cit.*, note 77.

84 *Szabó and Vissy v Hungary*, *op. cit.,* note 76.

85 *Mustafa Sezgin Tanrıkulu v Turkey*, Appliaction No. 27473/06, Judgment, 18 July 2017.

86 See: Syed, *op.cit.,* note 51, p. 166.

87 *Volodina v Russia*, Application No. 40419/19 (No. 2), Judgment, 14 September 2021.

88 In 2018, fearing for her safety, the applicant obtained a legal change of name. Her old name is used in the judgment to protect her safety.

impersonated her and used intimate photos to create fake profiles on social networks, put a GPS tracker in her purse, sent death threats via social media, and that the authorities did not effectively investigate her allegations.

Particularly interesting here is that the violation of the applicant's privacy (i.e., personal data) was not committed by the state, but by an individual (the applicant's ex-partner). The ECtHR found that Russian authorities violated Article 8 of the Convention in failing to fulfill their obligations under that provision to protect the applicant from serious abuse. In essence, the court took the view that, despite having mechanisms to prosecute the applicant's ex-partner, the authorities failed to conduct an effective investigation and identify and employ mechanisms to protect the applicant from repeated online harassment.[89]

4.2. Case-law of the CJEU

A search of the CJEU case-law by the terms 'data protection' and 'cybersecurity returns only two cases: *Schrems*[90] and *Natsionalna agentsia za prihodite*.[91] The latter is in proceedings before the CJEU after having been referred for a preliminary ruling. A search by the term 'cyber space' instead of 'cybersecurity' returns zero matches. Replacing the term 'cybersecurity' with the term 'national security' returns a significantly larger number of matches: 142, including the two abovementioned cases. This supports the above premise that for a long time the EU legislator, and consequently the CJEU, viewed cybersecurity through the lens of national security as only one of its elements. To draw conclusions from a sufficiently large sample pool, this paper will turn to analyzing the recent cases concerning the protection of personal data, which the CJEU examines through the lens of national security, but that by their nature concern cybersecurity. The cases in which the CJEU decided on the protection of personal data were referred to the CJEU by national courts. Important to note here is that – unlike the ECtHR – the CJEU has limited jurisdiction in the area of member states' security policy.[92,93] To begin our analysis, we first turn to the indispensable *Schrems*.

---

89 See the comment on the judgment and its importance for fighting violence against woman: *Centre for Women, Peace and Security*, [https://blogs.lse.ac.uk/vaw/landmark-cases/a-z-of-cases/volodina-v-russia-2019], Accessed 29 December 2022.

90 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559.

91 Case C-340/21 *Natsionalna agentsia za prihodite* (in proceedings).

92 See Art. 2(4) TFEU and Art. 72 TFEU.

93 Syed, *op.cit.*, note 51, p. 160.

In *Schrems*,[94] the CJEU was requested a preliminary ruling in the matter of the transfer of personal data for commercial purposes by a private company in an EU member state to a private company in a third country.[95] With its Decision 2010/87/EU, the Commission established standard contractual clauses for personal data transfer to third-country processors. *Schrems* concerns the validity of Decision 2010/87/EU. Regarding the request for judicial protection, the CJEU ruled that, contrary to Commission Decision 2016/1250, the ombudsperson mechanism provided for in the decision does not guarantee individuals a legal remedy before a body that offers protective measures essentially equivalent to those required by EU law, which could ensure both the independence of the mechanism-provided ombudsperson and the existence of rules enabling said ombudsperson to make decisions binding on the US intelligence services. For these reasons, the CJEU invalidated Commission Decision no. 2016/1250.[96]

In *Digital Ireland*,[97] the CJEU found that, in accordance with Directive 2006/24/EC[98] (Data Retention Directive), the rights under Articles 7 and 8 of the Charter are not absolute and that state interference is justifiable if it serves legitimate objectives such as combatting serious crime and international terrorism. However, the CJEU, after carrying out the proportionality test, invalidated Directive 2006/24/EC on grounds that it "did not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter." Further, the CJEU found that "it must therefore be held that Directive 2006/24/EC entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an in-

94 *Schrems, op. cit.,* note 90.

95 Maximillian Schrems, an Austrian national residing in Austria, had been a Facebook user since 2008. As with other EU residents, Mr. Schrems' personal data was transferred by Facebook Ireland in whole or in part to servers belonging to Facebook Inc. that are located on USA territory, where the data were also processed. Mr. Schrems submitted an application to the Irish supervisory authority essentially asking for a ban on those transfers. He claimed that the law and practices in the US do not guarantee a sufficient level of protection against access by public authorities to data transferred to that country. The application was rejected, inter alia, on grounds of Commission Decision 2000/5205 (Safe Harbor Decision) under which the US provides an adequate level of protection.

96 Schrems, *op. cit.,* note 90, paras. 197-202. See also: Press release of the CJEU No 91/20, Luxembourg, 16 July 2020.

97 See Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.

98 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105, p. 54–63.

terference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[99]

In one of the most recent cases, *Ligue des droits humains*,[100] the CJEU had the opportunity to rule on the validity of the EU Directive on Passenger Name Record (PNR) data.[101] Also called a booking file, PNR is reservation data pertaining to an individual or groups of travelers stored by airlines in their reservation and departure control databases. Under the PNR Directive, airlines are to transfer passenger data on flights to and from the EU to the passenger information department of the member state of destination or departure for the purpose of combating terrorism and serious crime. These data are stored for the potential subsequent assessment carried out by the competent authorities of the respective or other member state. The Belgian Ligue des droits humains filed a petition to the Belgian Constitutional Court for the annulment of the Belgian Act transposing the PNR Directive into Belgian law. The CJEU was requested a preliminary ruling in the matter of the validity and interpretation of the PNR Directive and the applicability of the GDPR.

The CJEU found that the PNR Directive clearly and seriously interferes with the rights guaranteed in Articles 7 and 8 of the Charter, in that it, inter alia, seeks to implement a continuous, untargeted and systematic surveillance regime, including the automated assessment of all airline passengers' personal data.[102] Although the CJEU validated the PNR Directive, in interpreting certain provisions of the Directive, it also set up fences around its application. A discussion of them would go beyond the scope of this work, but they are nonetheless worth referring to.[103]

In *Planet49*,[104] the CJEU interpreted the term 'consent' as defined under the Privacy and Electronic Communications Directive,[105] in conjunction with the Data

---

99 *Digital Ireland*, *op. cit.,* note 97, par. 65.

100 Case C-817/19 *Ligue des droits humains v Conseil des ministre* [2022] ECLI:EU:C:2022:491. The case was decided on 21 June 2022.

101 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJL 119.

102 See: *Ligue des droits humains*, *op.cit.,* note 100, par. 111.

103 *Ibid.,* see e.g. paras. 129, 157, 168, etc. For more details see: Press release of the CJEU No 105/22, Luxembourg, 21 June 2022.

104 Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* [2019] ECLI:EU:C:2019:801.

105 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337.

Protection Directive[106] and the GDPR. [107] The German Federation of Consumer Organizations contested before the German courts the German company Planet49's use of pre-ticked checkboxes in the company's promotional lottery for obtaining participants' consent for the setting of cookies whose purpose was data collection for Planet49's product advertising partner.

The CJEU found that the consent to store or access data through cookies installed on the website user's devices is invalid if given using a pre-ticked checkbox, regardless of whether the data in question is of a personal nature. Furthermore, the CJEU ruled that the service provider failed to inform the website user of the cookies' duration and any third parties' access to the cookies. The Court also took the view that Article 5(3) of the Privacy and Electronic Communications Directive is aimed at protecting users from invasion of privacy, regardless of whether the invasion targets personal data. It follows that 'consent' should not be interpreted differently if the data stored or viewed on the website user's devices is personal data.[108] Namely, EU law seeks to protect the user from any invasion of privacy, regardless of whether the data stored or viewed on the user's devices is personal data.[109]

5. CONCLUDING REMARKS

In these times of globalization and digitalization, the private lives of individuals are exposed to the public and privacy threats more than ever before. Firstly, the modern way of life increasingly requires the sharing of personal data (e.g. online shopping). Secondly, technology has enabled the creation of large databases of personal data, as well as their storage, connection and sharing. Thirdly, no longer is the state the only one encroaching on private data; large corporations and other entities are increasingly becoming party to it.[110]

With the digital economy's growth, companies are also collecting large amounts of customer data and analyzing them to learn about their habits and target them bet-

---

106 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

107 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 (General Data Protection Regulation) [2016] OJ L 119.

108 *Planet49*, *op.cit.,* note 104, paras. 63, 69 and 81.

109 See more in: Press release of the CJEU No 125/19, Luxembourg, 1 October 2019.

110 Schünemann; Baumann, *op. cit.,* note 4, pp. 190-193.

ter, and ultimately generate greater profit.[111] Personal data may also be breached by other individuals for a number of reasons.[112]

Clear from the above is the urgent need to protect the privacy of individuals, especially their personal data – an impossible feat without a sound legislative framework. Not to be overlooked is the national and EU courts' key role in personal data and privacy protection. In this demanding task, the courts must balance the right of individuals to personal data protection and privacy with other legitimate interests, such as national security.

For a long time, cybersecurity was associated with national security, with disregard of what 'secure' Internet means for individual users. It is safe to say that cybersecurity was angled more toward system(s) than individuals, i.e., system users. The 2019 EU Cybersecurity Act and subsequent legislation represent a normative shift in our conception of data ownership in the context of cybersecurity, putting the reins of personal information in the hands of the user instead of the service provider. Unfortunately, the positive legislative shifts at the EU level have yet to be implemented in a greater measure in the CJEU's practice and case-law.

As Brown puts it, it indeed is time to treat cybersecurity as a human rights issue.[113] But is it not also time for the ECtHR to consider cybersecurity as a human right *per se*– as a right to free and secure Internet for individuals*?* If so, at issue would then – instead of the protection of personal data in the context of cybersecurity – be two complementary autonomous human rights. Being a "living instrument" that the Convention is leaves room for the ECtHR to align its approach with the above proposal. Regrettably, as the analysis of its case-law has shown, the ECtHR still takes the traditional approach: human rights vs. national security/cybersecurity.

The differing case-law of the two European courts (ECtHR and CJEU) is in particular opposition to the protection of individuals' personal data in the context of cybersecurity. To exemplify, the ECtHR decision in *Big Brother Watch* is the first decision in which the court had the opportunity to rule on the legality of the international sharing of collected data. The ECtHR's approach to it is in complete contrast to the CJEU's position, which underlines the data-receiving third coun-

---

111 Schünemann; Baumann, *op. cit.*, note 4, p. 3. See also: Savin, A. (ed.), *EU Internet Law*, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2013, pp. 190-218.

112 Savin, *op. cit.,* note 111, p. 191. See case *Volodina v. Russia*, *op. cit.,* note 87, where the infringement on personal data in nature was committed by the applicant's ex-partner.

113 Brown, D., *It's Time to Treat Cybersecurity as a Human Rights Issue,* Human Rights Watch, 2020, [https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue], Accessed 5 January 2023.

tries' protective measures. Specifically, in *Schrems II*,[114] the CJEU annulled the so-called EU-US Privacy Shield[115] agreement that enabled transatlantic data transfers between the two countries that was in line with EU data protection requirements (the US surveillance system lacked adequate protective measures). The only difference between *Big Brother Watch* and *Schrems* is that the UK requested data from a third country, and not supply it. It remains unclear whether the ECtHR requires that adequate safeguards be in place in the receiving third country with which a Charter-contracting state shared the data. Per Zalnieriute, this ECtHR approach is ultimately reductive and dutiful, and angled at procedural safeguards more so than on the substantive legality or the actual effectiveness of the regime.[116]

The relation of the CJEU and the ECtHR has remained unchanged. In earlier research, the present authors found that the relationship of the two courts has been an oscillating one. The CJEU initially protected human rights as general principles of law, while referring to the ECtHR's case-law. Following the entry into force of the Charter, in a reasonably rational move, the CJEU began giving it precedence. This, however, began creating a schism between the two courts' positions. Their differing practices fail the reinforcing of human rights protection in the EU and complicate matters for the national (constitutional) courts. Additionally, the two courts refer to the case-law of the other only when it supports their own position.[117] It follows that the personal data protection standards of the EU are higher than those of the Council of Europe, i.e., that the scope of data protection in the case-law of the CJEU's is broader than that of the ECtHR.[118]

REFERENCES

BOOKS AND ARTICLES

1. Cherubini, F., *The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View of the Accession*, German Law Journal, Vol. 16, No. 6, 2015, pp. 1375-1386
2. Christou, G., *Cybersecurity in the European Union*, Palgrave Macmillan, London, 2016, pp. 87-118

---

114 Case C-311/18 *Schrems*, *op. cit.,* note 90.

115 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (notified under document C/2016/4176) [2016] OJ L 207.

116 Zalnieriute, M., *Big Brother Watch and Others v. the United Kingdom*, Am J Int L, 116(3), 2022, p. 589.

117 Petrašević; Duić, *op.cit.*, note 16, p. 228-229.

118 As found in the present authors' previous research, and the present analysis confirmed. See: Duić; Petrašević, *op. cit.,* note 16, p. 229.

3. Duić, D., *Common Security and Defence Policy and Cyber Defence*, in: Brill, A.; Misheva, K.; Hadji-Janev, M. (eds.), Toward Effective Cyber Defense in Accordance with the Rules of Law, IOS Press, Amsterdam, 2020, pp. 32-42
4. Duić, D., *The EEAS as a Navigator of EU Defence Aspects in Cyberspace*, European Foreign Affairs Review, Vol. 26, No. 1, 2021, pp. 101-114
5. Jakir, V., *Human Rights – With or without the internal market*, Zagreb, 2012, master thesis.
6. Kokott, J., Sobotta, C., *The Distinction between Privacy and Data Protection,* International Data Privacy Law, Vol. 3, No. 4, 2013, pp. 222-228
7. Lazowski, A.; Wessel, R.A., *When Caveats Turn into Locks: Opinion 2/13 on Accession of the European Union to the ECHR*, German Law Journal, Vol. 16, No. 1, 2015, pp. 179 – 212
8. Omejec, J., *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava*, Novi informator, Zagreb, 2013
9. Pavlova, P., *Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups*, Peace Human Rights Governance, Vol. 4, No. 3, 2020, pp. 391-418
10. Petrašević, T., Duić, D., *Direktiva o evidenciji podataka o putnicima (PNR) i zaštita podataka u EU,* in: Vukosav, J.; Butorac, K.; Sindik, J. (eds.), Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda, MUP, Policijska akademija, Zagreb, 2016, pp. 638-652
11. Petrašević, T., Poretti, P., *Pravo na suđenje u razumnom roku – postoji li (nova) praksa Suda Europske unije?*, Harmonius - Journal of Legal and Social Studies in south East Europe, Vol. 7, No. 1, 2018, pp. 187-199
12. Petrašević, T., *The relation of Human Rights and market freedoms in case law of the CJEU*, in: Primorac, Ž. ; Bussoli, C. ; Recker, N. (eds.), Economic and Social Development: 16th International Scientific Conference on Economic and Social Development "The Legal Challenges of Modern World", Varaždin/Split, 2016, pp. 142-150
13. Petrašević, T.; Duić, D., *Opinion 2/13 on the EU accession to the ECHR*, in: Vinković, M. (ed.), New Developments in the EU Labour, Equality and Human Rights Law, J. J. Strossmayer University of Osijek, Faculty of Law, Osijek, 2015, pp. 251-267
14. Petrašević, T.; Duić, D., *Standards of Human Rights Protection in the Domain of Personal Data Protection: Strasburg vs Luxemburg*, in: Sander, G. G.; Poščić, A.; Martinović, A. (eds.), Exploring the Social Dimension of Europe- Essays in Honour of Nada Bodiroga-Vukobrat, Verlag Dr. Kovač, Hamburg, 2021, pp. 215-231
15. Petrašević, T.; Kovačić Markić, L., *Položaj nacionalnih ustavnih sudova u primjeni mehanizma prethodnog postupka s posebnim osvrtom na Ustavni sud Republike Hrvatske*, in: Bačić, A. (ed.), Pravo i politika EU: stara pitanja, novi odgovori, HAZU, Zagreb, 2020, pp. 143-176
16. Savin, A. (ed.), *EU Internet Law*, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2013
17. Schünemann, W., Baumann, MO. (eds) *Privacy, Data Protection and Cybersecurity in Europe*, Springer, Cham, 2017
18. Syed, H., *Data protection rights & national security objectives: critical analysis of ECtHR and CJEU case law*, Nor. Am. Aca. Res., Vol. 2, No. 3, 2019, pp. 155-170

19. Wiśniewski, A., *The European Court of Human Rights and Internet-Related* Cases, Bialystok Legal Studies, Vol. 26, No. 3, 2021, pp. 109-133
20. Zalnieriute, M., *Big Brother Watch and Others v. the United Kingdom*, American Journal of International Law, Vol. 116, No. 3, 2022, pp. 585-592

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd [2020] ECLI:EU:C:2020:559
2. Case C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238
3. Case C-817/19 Ligue des droits humains v Conseil des ministre [2022] ECLI:EU:C:2022:491
4. Case C-340/21 Natsionalna agentsia za prihodite (in proceedings)
5. Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV [2019] ECLI:EU:C:2019:801
6. Press release of the CJEU No 125/19, Luxembourg, 1 October 2019
7. Press release of the CJEU No 91/20, Luxembourg, 16 July 2020
8. Press release of the CJEU No 105/22, Luxembourg, 21 June 2022

ECHR

1. *Guide to the Case-Law of the European Court of Human Rights: Data protection*, Council of Europe / European Court of Human Rights, 2022 (Updated on 31 August 2022)

Decisions:

1. *Airey v Ireland,* Application No. 6289/73, Judgment, 9 October 1979
2. *Big Brother Watch and Others v the United Kingdom,* Application Nos. 58170/13, 62322/14, 24960/15, Judgment, 13/09/2018; and *Big Brother Watch and Others v the United Kingdom,* Application Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment, 25 May 2021
3. *Cengiz and Others v Turkey,* Application Nos. 48226/10, 14027/112015, Judgment, 1 December 2015
4. *Centrum för Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021
5. *Delfi AS v Estonia,* Application No. 64569/09, Judgment, 16 June 2015
6. *Demir and Baykara v Turkey,* Application No. 34503/97, Judgment, 12 November 2008
7. *Dumitru Popescu v Romania,* Application No. 71525/01 (No. 2), Judgment [2007]
8. *Iordachi and Others v Moldova,* Application No. 25198/02, Judgment, 10 February 2009
9. *K.U. v Finland*, Application No. 2872/02, Judgment, 2 December 2008
10. *Klass and Others v Germany,* Application No. 5029/71, Judgment, 6 September 1978
11. *Liberty and Others v the United Kingdom,* Application No. 58243/00, Judgment, 1 July 2008

12. *Weber and Saravia v Germany,* Application No. 54934/00, Decision, 29 June 2006
13. *Youth Initiative for Human Rights v Serbia,* Application No. 48135/06, Judgment, 25 June 2013
14. *Mustafa Sezgin Tanrıkulu v Turkey,* Appliaction No. 27473/06, Judgment, 18 July 2017
15. *Roman Zakharov v Russia,* Application No. 47143/06, Judgment, 4 December 2015
16. *S. Marper v the United Kingdom,* Application Nos. 30562/04 and 30566/04, Judgment, 4 December 2008
17. *Szabó and Vissy v Hungary* App. No. 37138/14, Judgment, 12 January 2016
18. *Uzun v Germany,* Application No. 35623/05, Judgment, 2 September 2010
19. *Volodina v Russia,* Application No. 40419/19 (No. 2), Judgment, 14 September 2021

EU LAW

1. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security [2022] 7371/22
2. Charter of Fundamental Rights of the European Union [2012] OJ C 326
3. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (notified under document C/2016/4176) [2016] OJ L 207
4. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L 129I
5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, [2013] JOIN(2013) 1 final
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337
8. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105
9. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJL 119

10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194
11. Joint communication to the European parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN/2020/18 final
12. 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 (General Data Protection Regulation) [2016] OJ L 119
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151
14. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT [2021] OJ L 202
15. Treaty on the Functioning of the European Union (Consolidated version) [2016] OJ C 202

COUNCIL OF EUROPE

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) [2003]
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [1981]
3. Convention on Cybercrime (ETS No. 185) [2001]

UNITED NATIONS

1. United Nations, *General Assembly backs right to privacy in digital age,* [https://news.un.org/en/story/2013/12/458232], Accessed 30 December 2022
2. United Nations, High Commissioner for Human Rights, *The right to privacy in the digital age*, [https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age], Accessed 30 December 2022
3. United Nations, General Assembly, Resolution A/RES/68/167 on the right to privacy in the digital age, 18 December 2013
4. United Nations, High Commissioner for Human Rights, Resolution A/HRC/RES/32/13 on the promotion, protection and enjoyment of human rights on the Internet, 18 July 2016

WEBSITE REFERENCES

1. Freedom Online Coalition, *Aims and Priorities*, [https://freedomonlinecoalition.com/aims-and-priorities/], Accessed 25 November 2022

2. Brown, D., *It's Time to Treat Cybersecurity as a Human Rights Issue,* Human Rights Watch, 2020, [https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue], Accessed 5 January 2023
3. Centre for Woman, Peace and Security, [https://blogs.lse.ac.uk/vaw/landmark-cases/a-z-of-cases/volodina-v-russia-2019], Accessed 29 December 2022
4. Council of Europe, *Action against Cybercrime*, 2023, [https://www.coe.int/en/web/cybercrime], Accessed 5 January 2023
5. Council of the EU, *Cyber-attacks: Council extends sanctions regime until 18 May 2025*, 2022, [https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025], Accessed 5 January 2023
6. Douglas-Scott, S., *Opinion 2/13 on EU Accession to the ECHR*: *A Christmas Bombshell From the European Court of Justice*, U.K. Const. L. Blog, [http://ukconstitutionallaw.org], Accessed 30 December 2022
7. ENISA - European Union Agency for Cybersecurity, *About*, [https://www.enisa.europa.eu/about-enisa/about/], Accessed 5 January 2023
8. European Commission, *Building strong cybersecurity – Brochure*, 2019, [https://digital-strategy.ec.europa.eu/en/node/1500/printable/pdf], Accessed 5 January 2023
9. Gotev, G., *Court of Justice rejects draft agreement of EU accession to* ECHR, Euractiv, [http://www.euractiv.com/sections/eu-priorities-2020/court-justice-rejects-draft-agreement-eu-accession-echr-310983], Accessed 30 December 2022
10. Peers, S., *The CJEU and the EU's Accession to the ECHR: A Clear and Present Danger to Human Rights Protection*, EU L. Analysis Blog, [http://eulawanalysis.blogspot.com.es/2014/12/the-cjeu-and-eus-accession-to-echr.html], Accessed 30 December 2022
11. Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights,* Open-Democracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights/], Accessed 25 November 2022
12. *What is cybersecurity?*, [https://support.microsoft.com/en-us/topic/what-is-cybersecurity-8b6efd59-41ff-4743-87c8-0850a352a390], Accessed 25 November 2022
13. Freedom Online Coalition, *Why Do We Need a New Definition for Cybersecurity?*, [https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity], Accessed 25 November 2022

UDK 351.756:004
Original scientific paper

OF BIOMETRIC DOCUMENTS, DATABASES AND FREE MOVEMENT OF PERSONS IN THE EU*

Alessandra Lang, PhD, Associate Professor
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
alessandra.lang@unimi.it

ABSTRACT

Free movement of persons is a right recognised by the Treaty on the Functioning of the European Union (TFEU) for EU nationals (and their family members, irrespective of their nationality), and is one of the rights related to EU citizenship. Being an EU national is the qualifying element to benefit from the free movement regime, which is more favourable than the immigration regime otherwise applicable to foreigners. In order to prove one's nationality, identity cards and passports play a central role. The issuance of these documents is regulated by national law. Over the last 20 years, EU law has intervened in this area with the aim of strengthening the document security. In 2004, the EU institutions passed a regulation on biometric passports and in 2019 a regulation on biometric identity cards. From now on, the facial image and fingerprints data of the holder are kept in the storage medium in these documents. The reasons for the introduction of biometric data lie in preventing the falsification of the document and the fraudulent use of authentic documents. On the one hand, the techniques used to preserve and protect the data make these documents more difficult to forge. On the other hand, the presence of biometric data creates a reliable link between the holder and the person who owns the document, thus making it easier to identify the person, and more difficult to use the document fraudulently by those who are not the real holder.

Meanwhile, the EU is promoting the interoperability of the many databases established overtime. Interoperability connects different databases and makes the data stored in them searchable and accessible to a wider range of authorities and for other purposes than those for which they are collected. Biometric data, such as facial images and fingerprints are stored in many databases.

The paper will sketch out the interference of the two issues (biometric documents and databases) in relation to the free movement of persons, in order 1) to map the instances in which

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

controls on biometric documents of EU nationals or family members lead to search in the databases, and 2) to assess the impact that the very existence of biometric documents and databases can have on the fundamental rights of individuals.

***Keywords**: biometrical documents, databases, EU citizenship, EU nationals, fingerprints, free movement of persons*

1. INTRODUCTION

Free movement of persons allows Union citizens and their family members to travel between Member States and to move to a different Member State from their country of origin, thanks to their nationality. Identity documents are important because they are the primary way of proving the holder's nationality. In recent years, the European Union has stipulated that any identity documents (passports and identity cards) issued by Member States must contain biometric data. This article seeks to explore the basis for this legislation and to assess whether it provides reliable guarantees that the biometric data collected for inclusion in identity documents is not stored in databases.

2. IMPORTANCE OF IDENTITY DOCUMENTS FOR FREE MOVEMENT OF PERSONS

Identity documents have an important function in the free movement of persons because they are the primary way of proving the identity and citizenship of their holders. Citizenship, in turn, is the determining factor for applying the EU laws on citizenship rights, first and foremost among which is the right to free movement of persons. This right is now enshrined in Article 21 TFEU and Article 45 CFREU, and is regulated by Directive 2004/38.[1] Free movement means that Union citizens have the right to leave their home State and enter and reside in another Member State. Correlatively, Member States are obliged to grant Union citizens rights of exit, entry and residence under the conditions laid down in EU law. This right is neither unconditional nor unlimited. EU law itself provides that Union citizens must meet the conditions required to exercise the rights attached to free movement. These conditions are that individuals claiming free movement rights must be Union citizens, proven by an identity document, and must, for periods of residence of longer than three months, prove that they fall into one of the

[1] Directive 2004/38/EC of the European Parliament and of the Council on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77. Guild, E.; Peers, S.; Tomkin, J. (eds.), *The EU citizenship directive: a commentary*, Oxford University Press, Oxford, 2nd ed., 2019.

following categories: workers or self-employed persons, students with sufficient resources and sickness insurance, persons who are economically self-sufficient (because they have sufficient resources and sickness insurance) or family members of a Union citizen who falls into one of the three categories mentioned above. On the other hand, free movement rights may be restricted by States on grounds of public policy, public security and public health, subject to the safeguards provided for in EU law.

Directive 2004/38 sets out the administrative formalities that the host State may require Union citizens to fulfil. Specifically, a Union citizen who is intending to reside for longer than three months may be required to register with the relevant authorities. In this way, the host State can verify that the Union citizen meets the substantive requirements laid down in EU law and can release a residence certificate.

As far as treatment is concerned, the Directive provides that Union citizens are entitled to equal treatment with host State nationals, albeit with certain restrictions (art. 24). After five years of legal and continuous residence, Union citizens acquire the right of permanent residence (Art. 16), which sees an improvement in their legal status. For example, the right of permanent residence is no longer conditional on meeting the criteria for periods of residence of more than three months (that is, being a worker, a student or economically self-sufficient), equal treatment applies without restrictions of any kind and Union citizens qualify for enhanced protection against expulsion.

How the host State treats non-citizens depends primarily on citizenship. Applying the rules on free movement or immigration depends on the person's citizenship above and beyond any personal characteristics. It comes as no surprise, therefore, that some people seeking to take advantage of the more favourable free movement rules are prepared to engage in illegal behaviours in order to obtain a document certifying that they hold Union citizenship, such as using counterfeit documents or fraudulently using genuine documents. The Member States are very concerned about this risk, and this may explain why there is an increasing focus on biometric documents, the subject-matter of this article.

As far as identity documents are concerned, Directive 2004/38 states that possession of a passport or identity card proving the holder's nationality is a necessary and sufficient condition for exercising the right to leave the country of origin or residence (Article 4(1)),[2] to enter another Member State (Article 5(1))[3] and to

[2] The article goes on to say that States cannot impose any exit visa or equivalent formality.

[3] This article also prohibits States from imposing entry visas or equivalent formalities. An identity card is therefore a travel document, in the same way as a passport, and not just an identity document.

reside in another Member State for up to three months (Article 6(1)) and is a necessary but not sufficient condition for a period of residence of more than three months (Article 8(3)). Member States are obliged to issue passports or identity cards to their citizens.[4] Issuing documents is a matter of national competence, but States must do this in a way that does not undermine the rights that Union citizens derive from EU law. Since the prerequisite for exercising the right is possession of a document that only national authorities can issue, the Court of Justice considers that a State cannot impose conditions which, if not satisfied, would entitle it to refuse to issue an identity document to its citizens.[5]

The State which issued the identity document is also obliged to allow the holder who has been expelled from another Member State to re-enter its territory, without being able to raise any objections over the validity or authenticity of the document (Article 27(4)).

The Court of Justice has clarified the *ratio* and scope of the requirement to hold a passport or identity card. It has stated that free movement is a right of Union citizens and that States may demand proof of citizenship. Possession of an identity document is an administrative formality that facilitates free movement by making it easier to identify the beneficiaries.[6] Lack of a valid passport or identity card may be sanctioned as an administrative offence, but the State cannot claim that the person is not entitled to free movement. Since the right to free movement is a consequence of citizenship, and passports and identity cards are merely means of evidence, the Court concludes that the State must give the person every opportunity to prove their identity in some other way.[7] Accordingly, the State should also

---

Passports are travel documents accepted by States as a matter of comity (see Hagedorn, C., *Passport*, Max Planck Encyclopedia of Public International Law, 2008, para. 7), whereas identity cards fulfil this function between States that accept them, usually in accordance with an international agreement but also (as in this case) under EU law.

4 Similar provisions had previously been included in Article 2(2) of Directive 68/360 on the free movement of workers and Article 2(2) of Directive 73/148 on the right of establishment and the free movement of services, whereas the directives issued in the 1990s extending free movement to students (Directive 93/96), pensioners (Directive 90/365) and economically self-sufficient persons (Directive 90/364) contained no provisions to that effect.

5 See, in particular, Case C-490/20 *Stolichna obshtina, rayon 'Pancharevo'* [2021] ECLI:EU:C:2021:1008, par. 45.

6 Case C-35/20 *A* [2021] ECLI:EU:C:2021:813, par. 53.

7 Case C-215/03 *Oulane* [2005] ECLI:EU:C:2005:95 par. 23, which cites as precedent case C-459/99 *MRAX* [2002] ECLI:EU:C:2002:461, par. 62, a statement later codified in Article 5(4) of Directive 2004/38. So, while the directive sets out this principle in cases where a Union citizen does not have any documents at the time of entry, under the *Oulane* case law, a similar principle applies when the person is already in the country and must prove their right of residence.

accept documents that are not valid for leaving the country[8] or other documents that are means of evidence of identity under national law (such as driving licences in some States).

EU law requires States to recognise the validity of travel and identity documents issued by other Member States, unless there are justified reasons to believe that a certain document has been falsified.[9] A falsified document may constitute a case of fraud which, under Article 35 of Directive 2004/38, justifies the refusal of free movement rights.[10]

Family members of Union citizens, regardless of their nationality, also benefit from these special legal rules. They enjoy freedom of movement in order to enable their relative, a Union citizen, to enjoy family unity even if that person moves to another Member State. The right to family reunification (within its broad meaning of the right to accompany a relative or to be reunited with a relative) has, since the very beginning of free movement, been portrayed first and foremost as a right for migrant workers and then as a right for Union citizens. It follows that family members do not enjoy free movement rights independently but only if they are travelling and residing with a Union citizen or they move to reunify with a Union citizen. In these cases, their legal status is equivalent to that of a Union citizen and they are exempt from the less favourable immigration rules. The discriminating factor between applying free movement of persons and immigration law is not the person's nationality but rather their family ties. For this reason, States want, on the one hand, to exercise a certain control over family members and, on the other hand, to counter behaviour such as sham marriages or adoptions as a means of pre-establishing family ties.[11] Directive 2004/38 contains a number of specific provisions to reassure the concerns of the Member States: firstly, the only

---

8 Case C-376/89 *Giagounidis* [1991] ECLI:EU:C:1991:99, par. 16.

9 Case C-202/13 *McCarthy* [2014] ECLI:EU:C:2014:2459, par. 58. The principle, expressed in relation to the residence cards of family members (see below), can also be extended to identity documents.

10 "In the context of the Directive, fraud is likely to be limited to forgery of documents or false representation of a material fact concerning the conditions attached to the right of residence": Communication from the Commission to the European Parliament and the Council on guidance for better transposition and application of Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States, COM/2009/313 final.

11 Pursuant to Article 35 of the Directive, Member States can deny or revoke the right of residence in these cases. See Commission Staff Working Document, Handbook on addressing the issue of alleged marriages of convenience between EU citizens and non-EU nationals in the context of EU law on free movement of EU citizens, SWD/2014/284.

travel and identity document stipulated by the directive is a passport and not a passport as well as an identity card;[12] secondly, entry into the State may be subject to possession of a visa, regardless of the family member's place of residence, in cases where EU or national law requires this for entry from a third country (Article 5(2)).[13] There is, however, an exception, which benefits family members who hold a residence card, in other words family members who are resident with their spouse in a Member State of the European Union, having exercised their right to free movement.[14] Hence the importance of a residence card and the fears of falsification or fraudulent use which will be discussed further below. Thirdly, exercise of the right of residence for family members is subject to the performance of more onerous formalities than those existing for Union citizens. These include applying for and being issued with a residence card (and not just registering with the national authorities), as a means of further checking someone's identity and the potential danger that person poses, albeit that a residence card does not give rise to a right of residence but is merely of a declaratory nature.[15]

3. BIOMETRIC DOCUMENTS

Despite the importance of identity documents for free movement of persons, the rules governing identity documents have remained within the competence of the Member States. That is not to say that the Union has had no involvement in this area. In the 1980s, a uniform passport, largely symbolic in value, was established in order to create an outward and common mark of citizenship.[16] In the aftermath of the 9/11 attacks, the Western world felt the need for increased security, resulting in more extensive checks on those entering the country. The terrorist threat came

---

12 For exit (Article 4(1)), entry (Article 5(1)), residence of less than three months (Article 6(2)) and residence of more than three months (Article 10). The directive is not therefore the basis for recognition of identity cards as a travel document into and within the Union.

13 These are the cases covered by Regulation 2018/1806, which lists the States whose nationals must be in possession of visas when crossing the external borders including for short-stay visits. Ireland is the only State not bound by the Regulation, as it does not participate in the Schengen acquis. States are obliged to grant a visa to the family member, who must only apply for a short-stay visa, even if the intention is to stay for longer: Case C-157/03 *Commission v Spain* [2005] ECLI:EU:C:2005:225, par. 38.

14 Article 5(1) mentions only a residence card issued for a period of residence of more than three months, and not a permanent residence card, which is issued to the family member after five years of legal and continuous residence in accordance with Article 20. However, in Case C-754/18 *Ryanair Designated Activity Company* [2020] ECLI:EU:C:2020:478, par. 38, the Court stated that a permanent residence card also exempts a person from possessing a visa, rejecting the formalistic arguments put forward by the State concerned.

15 Case C-246/17 *Diallo* [2018] ECLI:EU:C:2018:499, par. 48.

16 Resolution of the Representatives of the Governments of the Member States of the European Communities, meeting within the Council 1981 [1981] OJ C 241/1. See Herting Randall, M.; Hänni, D.; *European Passport*, Max Planck Encyclopedia of Public International Law, 2019.

from outside and had to be stopped from entering. Leading the way, of course, was the United States, which introduced biometric passports and demanded that everyone entering the country must have one.[17] The European Union followed in its footsteps, so as to enable EU citizens to enter the United States. The inclusion of biometric data (facial image and fingerprints),[18] firstly in travel documents and later in identity documents, is justified by the need to make documents more secure (less falsifiable) and identity theft (preventing the use of another person's document) more difficult.[19] Biometric data is interesting because it can be taken from practically anyone, the technology for collecting, storing and reading it is well developed and biometric data is characterised by a certain (albeit not absolute) stability over time, which means that it can be compared with outcomes that are considered broadly reliable.

The biometric documents governed by EU law which will be considered here are passports, identity cards and residence cards of family members of Union citizens. The first two are both travel documents and identity documents.[20] Residence cards are neither one nor the other but when combined with a passport, their holder is treated as a Union citizen when crossing an external border, either coming in or going out (see below) and is exempt from the need to obtain a visa to cross the internal borders.

3.1. Biometric passports

Regulation 2252/2004,[21] amended by Regulation 444/2009[22] (containing highly appropriate amendments, as discussed in section 5.1.1), covers biometric pass-

---

17 Torpey, J., *The invention of the passport: surveillance, citizenship, and the state*, Cambridge University Press, Cambridge, 2018, pp. 195 - 206.

18 For a discussion on the technical and legal meaning of the notion, as well as on the different use of terms between biometric experts and data protection lawyers, see Jasserand, C., *Legal Nature of Biometric Data*: *From 'Generic' Personal Data to Sensitive Data*, European Data Protection Law Review, Vol. 2, No. 3, 2016, pp. 297-311.

19 However, it is debatable that biometric data makes documents more difficult to falsify: see Baechler, S., *Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?*, European Journal on Criminal Police and Research, Vol. 26, 2020, pp. 379 – 394.

20 At the same time, the EU is working on digital identity to access goods and services: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73. Since this subject is unrelated to travel or identity documents, it will not be discussed in this paper.

21 Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1.

22 Regulation (EC) No 444/2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and

ports. The Regulation does not establish a common model (which already exists) but merely provides that passports issued by Member States must contain a facial image and two fingerprints (Article 1), collected by authorised staff (Article 1a) and stored on a highly secure storage medium in the passport (Article 1). Technical characteristics are regulated through the Commission's implementing acts (Article 5). The Regulation also provides that children under the age of 12 years and persons for whom fingerprinting is impossible are exempt from the requirement to give fingerprints (Article (1)(2a)). The passport contains only the machine-readable information provided for in the Regulation or under national legislation (Article 4(2)). Access to biometric data is only permitted to verify the authenticity of the document and the identity of the holder (Article 4(3)). The Regulation does not stipulate which authorities may access this data but states that this is determined by the Member States (recital 4).

The Regulation does not establish the conditions for issuing passports or the data that must or may be contained in such documents. This is left to the discretion of the Member States, although reference can be made to ICAO Document 9303, which aims to standardise the information contained in travel documents in order to make them machine-readable.[23] According to the Court of Justice, the Regulation requires that the machine-readable biographical data page of passports issued by Member States must comply with the specifications for machine-readable passports laid down in Part 1 of ICAO Document 9303 and must satisfy all of the compulsory specifications provided for therein.[24] Thanks to the reference made by the Regulation, ICAO Document 9303 thus becomes binding on the Member States.[25]

travel documents issued by Member States [2009] OJ L 142/1.

23 The International Civil Aviation Organization (ICAO) is responsible for ensuring the orderly and safe development of international civil aviation, in particular through the adoption of international standards and recommendations, which may also include immigration formalities (Article 37(i), Convention on International Civil Aviation, Chicago, 7-12-1944). Document 9303 is one such recommendation. Pursuant to Article 23 of the Chicago Convention, States undertake to enact, where they deem this appropriate, immigration regulations that are consistent with ICAO recommendations. If States consider that they can comply with ICAO recommendations, they must, under Article 38, notify the ICAO of the differences between their own regulations and the ICAO recommendations. Abeyratne, R.I.R., *The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject*, Annals of Air and Space Law, Vol. 17, Part 2, 1992, at 1, points out that machine-readable documents have been envisaged as a tool to facilitate international air transport and tourism; hence the role played by ICAO.

24 Case C-101/13 *U* [2014] ECLI:EU:C:2014:2249, paras. 23-24.

25 Hornung, G., *Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues*, European Public Law, Vol. 11, 2005, p. 504.

3.2. Biometric identity cards

In 2019, the EU established a uniform format for identity cards[26] on which the holder's biometric data is stored. Without affecting the obligation to hold an identity card (applicable in all Member States except Denmark), the Regulation requires States to use the harmonised format when issuing documents and to progressively withdraw documents with a different format.[27] The format to be used is not brand new but is the same as that previously provided for in Regulation 1030/2002,[28] to which must be added "the two-letter country code of the Member State issuing the card, printed in negative in a blue rectangle and encircled by 12 yellow stars" (Article 3(4)). It should be noted that Regulation 1030/2002 concerns residence permits, which are essential for managing immigration policy but whose function is not comparable to an identity card and they are not normally used on their own but always accompanied by a passport.

Regulation 2019/1157 is very similar to Regulation 2252/2004. The inclusion of biometric data is justified for the same purposes, namely to make it more difficult to falsify documents and to use genuine documents fraudulently (recital 18) and access to data is only allowed for the same purposes (Article 11(3)).

Just like the Regulation on passports, this Regulation provides that identity cards issued by Member States must include a highly secure storage medium containing a facial image and two fingerprints (Article 3(5)) collected by authorised staff (Article 10(1)), according to procedures that respect fundamental rights (Article 10(2)). The Regulation also provides for exemptions from the requirement to give fingerprints (for children under the age of 6 years, a limit which States may raise to 12 years, and for persons in respect of whom fingerprinting is impossible: Article 3(7)). But unlike for passports, the Regulation on identity cards lays down certain rules on the format of the document. It states, firstly, that the specifications set out in part 5 of ICAO Document 9303 apply to the data elements included

---

26 Regulation (EU) 2019/1157 of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [2019] OJ L 188/67.

27 The explanatory memorandum accompanying the proposal for a regulation states that there are at least 86 different formats of identity cards: Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement SWD(2018) 110, p. 9.

28 Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals [2002] OJ L 157/1, as amended by Regulation No 2017/1954 [2017] OJ L 286/9.

on identity cards (Article 3(2)) and, secondly, that their format must be consistent with Regulation 1030/2002. Additional technical specifications may be established through the Commission's implementing acts (Article 14). The period of validity is also harmonised: between a minimum of 5 years and a maximum of 10 years (Article 4).

Access to biometric data is only permitted to verify the authenticity of the document and the identity of the holder (Article 11(6)). The Regulation does not stipulate which authorities may access this data as this is to be defined by the Member States. Unlike with the Regulation on passports, Member States must communicate the updated list annually to the Commission for publication purposes (Article 11(7)).

3.3. Residence cards of a family member of a Union citizen and permanent residence cards

Regulation 2019/1157 sets out the uniform format for the residence card by extending the scope of Regulation 1030/2002 on residence permits issued to third-country nationals who do not enjoy free movement rights (Article 7).[29] As far as biometric data is concerned, the residence card must contain a facial image and two fingerprints. Children under the age of 6 years and persons in respect of whom fingerprinting is physically impossible are exempt (Article 4-ter).

Articles 10 and 11 of Regulation 2019/1157, the relevant provisions of which are mentioned in the previous paragraph, also apply to residence cards.

4. WHEN AND IN WHAT CONTEXTS BIOMETRIC DOCUMENTS ARE CHECKED

Directive 2004/38 allows (but does not require) States to check, using documents, the nationality of beneficiaries of free movement of persons when completing the administrative formalities necessary for exercising free movement. But more generally, Union citizens (and their family members) will use their identity documents in their dealings with public or private authorities when carrying out the various formalities that are necessary or useful for living in a complex society. Examples include: dealing with tax authorities, paying taxes, dealing with social security agencies, accessing benefits, dealing with health authorities, receiving healthcare

[29] Article 5 of Regulation 1030/2002 states that it does not apply to third-country nationals who are family members of a Union citizen exercising their right to free movement. However, as the explanatory memorandum accompanying the proposal for a regulation states, some Member States were already using the residence permit format for residence cards.

benefits, dealing with banks, opening and managing a current account, dealing with private individuals, signing a tenancy agreement, and so on and so forth.

Instead, EU law requires national authorities to check documents, including those of Union citizens, at the time of crossing external borders, whether entering or exiting.

Systematic checks on the identity and travel documents of Union citizens at external borders (entering and exiting) was imposed by an amendment to the External Borders Code in 2017.[30] Previously, Union citizens were subject to less detailed checks to ascertain their nationality indicated in their travel document. Systematic checks are carried out when crossing external borders, that is to say those of a Schengen Area State[31] with a third country, when crossing borders between two Member States if internal border controls are still in place,[32] or if such controls have been reintroduced.[33]

This has been prompted by the terrorist threat posed by foreign terrorist fighters, which has brought about changes aimed at restricting the rules in force.[34] The term "foreign terrorist fighters" means nationals of a Member State who had travelled to the Middle East to join ISIS and who, after receiving training, returned to their home State supposedly to commit terrorist attacks. Although some of these individuals were checked when re-entering the European Union, they were not intercepted and went on to commit terrorist acts. The solution devised to counter the threat was to require border guards to carry out systematic database checks on all documents and names of individuals presenting themselves at external borders, whether entering or leaving, putting an end to the more favourable arrangements previously enjoyed by Union citizens.

The new Article 8 of the Borders Code, as amended by Regulation 2017/458, requires national authorities to carry out checks on the documents of all Union

---

30 Regulation 2017/458 of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L 74/1.

31 Recall that the Schengen Area comprises 26 Member States (with the exception of Ireland) and 4 third countries (Iceland, Liechtenstein, Norway and Switzerland).

32 This situation occurs in relation to the borders in Bulgaria, (Croatia until March 2023), Cyprus, and Romania.

33 States may, under certain circumstances and conditions, reintroduce controls at one or more internal borders.

34 This is very clear from the Commission proposal COM/2015/670. On this phenomenon, see, generally, De Guttry, A.; Capone, F.; Paulussen, C., *Foreign fighters under international law and beyond*, T.M.C. Asser Press, The Hague, 2016; De Coensel, S., *Terrorists on the move: a Legitimacy test of the Criminal Law approach on foreign fighters in Western Europe*, European Criminal Law Review, Vol. 10, No. 2, 2020, pp. 185 - 217.

citizens to verify that they are not counterfeit or stolen, and checks on persons to verify that they do not represent a threat to public policy or national security. To that end, the border guards consult the following databases: SIS II, SLTD (Interpol's Stolen and Lost Travel Documents database), national databases containing information on stolen, misappropriated, lost and invalidated travel documents. Checks on persons are carried out by consulting the SIS and "other relevant Union databases", including national and Interpol databases. Where there are doubts as to the authenticity of the document or the identity of the person, the border guards will verify at least one of the biometric identifiers integrated into the passport in accordance with Regulation 2252/2004. The article goes on to state that "where possible, such verification shall also be carried out in relation to travel documents not covered by that Regulation". This leaves the door open for verification of the biometric identifiers integrated into identity cards under Regulation 2019/1157 (following the 2017 amendment).

The arrangements briefly described above also apply to family members of Union citizens when exercising free movement of persons, in other words when they present themselves at an external border together with a Union citizen or in order to join a Union citizen. In other cases, they are subject to the same rules as third-country nationals, and checks at external borders are also designed to ascertain that they meet the requirements for entering or leaving the Union.

Systematic checks could lead to a refusal of entry. This measure must be justified on the basis of Directive 2004/38, as is evident from the recitals of Regulation 2017/458 (recital 15: "This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council"). The Directive applies to the entry of Union citizens into a State of which they are not nationals. But the entry of Union citizens into their country of origin lies outside of its scope.[35]

Entry could be refused for reasons to do with the document or the person. As far as the former is concerned, Article 35 of the Directive allows States to deny any right under the Directive in the case of fraud. As regards the latter, the Directive allows States to restrict rights of entry and residence on grounds of public policy and public security. Any decision restricting one of the free movement rights must be justified by the danger posed by the personal conduct of the individual concerned. In addition, the Directive provides procedural safeguards: any decision restricting free movement rights must be duly substantiated, notified to the individual concerned in writing, and amenable to judicial review.

[35] With the exception, which cannot be further discussed here, of Union citizens returning to their country of origin after exercising free movement of persons in another Member State.

However, systematic checks may also lead to other measures, depending on the type of alert that the database search returns. A useful read is the "Practical Handbook for Border Guards",[36] which outlines how border guards are expected to behave. Of particular interest is the action to be taken for the purposes of discreet or specific checks, pursuant to Article 36 of Council Decision 2007/533/JHA, because it allows border guards to collect further data on persons.

5. LEGITIMACY OF COLLECTING, STORING AND PROCESSING BIOMETRIC DATA IN TRAVEL AND IDENTITY DOCUMENTS

By using biometric data, it is possible to carry out two separate operations: identity authentication and identification. Identity authentication is about ascertaining whether the person holding the document is the same person to whom the document was issued and whose images are stored on the document, by comparing two images: the one on the document and the one taken of the person at that precise moment. This operation does not require the creation of databases but merely offline access to the storage medium placed on the document. Identification is about identifying the biometric data, in other words giving a name and an otherwise unknown identity to the person to whom the biometric data belongs. This operation requires comparing the biometric data to be identified with other biometric data that may be stored in databases.

The basis for each of the operations will be examined separately, relying mainly on primary sources, that is the letter of the relevant EU legislation.

5.1. Legitimacy of storing biometric data in documents

5.1.1. Passports

The Court of Justice has had the opportunity to rule on the legitimacy of including biometric data in passports,[37] with a preliminary ruling that merits being examined in greater depth.

The national proceedings concerned, on a factual level, the refusal by the competent national authority to issue a passport to the applicant, who refused to have his fingerprints taken, and, from a legal perspective, the validity of Regulation

[36] Annex to Commission Recommendation C(2019)7131 establishing a common "Practical Handbook for Border Guards" to be used by Member States' competent authorities when carrying out the border control of persons and replacing Commission Recommendation C(2006) 5186.

[37] Case C-291/12 *Schwarz* [2013] ECLI:EU:C:2013:670.

2252/2004, in the part where it requires that fingerprints must be taken in order for a passport to be issued. The applicant argues that the Regulation is vitiated by procedural defects (argument rejected by the Court and not of particular interest here) and infringes his fundamental rights. The Court examines this second ground at length and starts from the premise that taking fingerprints constitutes an interference with private life (Article 7 CFREU) and storing them is harmful to the protection of personal data (Article 8 CFREU), since the enjoyment of both rights is restricted (paragraph 30). The Court then considers whether there is a justification for this restriction. Having stated that the consent of the individual concerned cannot be inferred from their application for a passport, because that document is essential for travel (paragraph 32), the Court then goes on to examine the issue through the spectrum of Article 52(1) CFREU,[38] which allows for limitations on fundamental rights provided that a number of conditions are met.

The conditions that the Court considers when assessing whether a limitation of rights is justified are as follows: (a) the limitation must be provided for by law, (b) it must pursue an objective of general interest, (c) it must respect the essence of the rights, (d) it must be proportionate to the objective pursued, and (e) it must be necessary.[39] The Court examines each of these conditions in turn, adopting an approach that is at times vague but nonetheless substantially coherent, which will be summarised here.

(a) A limitation of rights is possible if it is provided for by law, and a regulation is an act that meets that requirement (paragraph 35).

(b) The objective pursued must be one of general interest. Here, the Court does not identify the aim of the regulation directly from the recitals but infers this from the aims that the regulation seeks to pursue. The recitals state that the rules governing biometric passports have two aims: to prevent the falsification of documents and to prevent the fraudulent use of a genuine document. These aims do not seem to fulfil the definition of objectives of general interest. Instead, they are intermediate objectives with respect to the objective that the Court considers to be the general objective recognised by the Union (paragraph 38), namely that of

[38] The benchmark for assessing the legitimacy of restricting fundamental rights is therefore primary law. At the time of the ruling, the legislation in force was Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31, which did not contain specific provisions on the processing of biometric data.

[39] This approach is taken from Article 52 CFREU and is consistent with the case law of the Court of Justice. See Lock, T., *Article 52 CFR*, in: Tomkin, J.; Klamert, M.; Kellerbauer, M. (eds.), EU Treaties and the Charter of Fundamental Rights: Digital Pack: A Commentary, Oxford University Press, Oxford, 2019

"prevent[ing], *inter alia*, illegal entry into the European Union" (paragraph 37). This general objective seems to this author to be traceable to the legal basis of the Regulation, Article 62(2)(a) TEC, which gave the institutions the competence to adopt measures on the checks to be carried out on persons at external borders, which are certainly not an end in themselves but the means to prevent illegal entry.

(c) According to the Court, which does not elaborate much on this point, the limitation respects the essence of fundamental rights, insofar as the opposite is not proven (paragraph 39).

(d) More detailed are the Court's discussions on the proportionality of the limitation to the aims pursued, in the sense that this must be appropriate for attaining the aims and must not go beyond what is necessary to achieve them. As regards whether the limitation is appropriate for attaining the specific aims of the regulation, namely to prevent the falsification of documents, the Court answers in the affirmative because this is *in re ipsa*: falsifying a biometric document is undeniably more difficult than falsifying a non-biometric document. In its assessment of the suitability of biometric passports for preventing fraudulent use of a genuine document, the Court discusses the applicant's argument that the margin of error when comparing fingerprints is too high to conclude that the document is fit for purpose, such that persons fraudulently using a document could be allowed entry and persons using a genuine document could be denied entry (paragraph 42). The Court responds not by contesting the merits of the argument but by minimising its scope: identification mistakes do occur but they are not so serious as to make the document unsuitable. Cases of mismatching do not negate the fact that illegal entries are lower compared with situations where there is no possibility of carrying out checks (paragraph 43). If the fingerprint comparison reveals that the fingerprints do not match, this does not mean that the person concerned will be refused entry but that an additional manual check, as specified in the final sentence of Article 4(3), will be carried out to identify the person concerned and verify their right of entry (paragraph 44). Note that this provision was added by Regulation 444/2009. The original version did not contain any provision to that effect, with all the risks of abuse that this could entail.

(e) The Court then states that the limitation of fundamental rights is necessary insofar as it does not go beyond what is necessary to achieve the aim, since fingerprinting is not an operation of an intimate nature (paragraph 48). In addition, measures that are equally effective and interfere less with the rights protected are not available. The only measure that can be considered is iris recognition, a procedure that the Court considers equivalent in terms of interference with rights at the time of the image is collected, but less effective in preventing fraudulent use

of passports, because the technology required is more expensive and the margin of error is no lower than for fingerprints (paragraph 52). Finally, the processing of fingerprints stored in the document must not go beyond what is necessary to achieve the aim pursued. According to Article 4(3) of the Regulation, the legitimate use of fingerprints is strictly limited to the aims pursued (verifying the authenticity of the passport and the identity of the holder) and is restricted to authorised staff.

5.1.2. Identity cards

The Court of Justice has not yet had the opportunity to rule on the legitimacy of collecting, storing and using fingerprints in identity cards and residence cards, although a number of references for a preliminary ruling are pending.[40]

To attempt an answer, it is possible to apply the same arguments developed by the Court in *Schwarz* as regards passports to identity cards and examine whether legitimacy can be based on consent or on the existence of grounds for justification for interference with fundamental rights under Article 52 CFREU.

Consent cannot form the basis for interference, because possession of an identity card is compulsory in almost all States and the applicant cannot choose whether or not to apply for one. If the Court has stated that consent cannot be presumed from a passport application, the same applies to an identity card.

Considering instead the arguments based on Article 52 CFREU, it can be stated first and foremost that interference is provided for by law, as this is specified in a regulation.

As regards the objective of general interest recognised by the Union, it seems difficult to argue that the objective identified by the Court for passports, namely to prevent unlawful entry into the EU, can also apply to identity cards. This is because there is nothing in the legal basis of the Regulation that concerns the control of external borders. Unlike Regulation 2252/2004, which is based on Article 62(2)(a) TEC, now corresponding to Article 77 TFEU, Regulation 2019/1157 finds its legal basis in Article 21(2) TFEU. This article allows the institutions to adopt provisions to facilitate the exercise of rights connected with the free movement of persons, in the absence of any other legal basis. The choice of this legal basis deserves some consideration. At first glance, it may be assumed that there is another, more suitable provision, Article 77(3), which authorises the institutions, once again in the absence of a more appropriate legal basis, to adopt provisions

[40] Cases C-61/22 [2022] OJ C 213/22, and C-280/22 [2022] OJ C 318/22.

concerning identity cards and passports which are necessary for the exercise of the rights referred to in Article 20(1) (i.e. free movement).[41] The exact scope of the two provisions is not self-evident. From a procedural point of view, the choice between the two provisions is not without consequences. Article 77 falls within the Area of Freedom, Security and Justice, and acts adopted on this basis are not binding on Denmark and Ireland.[42] In addition, Article 77(3) provides that the Council shall act unanimously after consulting the European Parliament, in accordance with a special legislative procedure in which the role of the Parliament is less incisive than under the ordinary legislative procedure provided for in Article 21(2).[43]

Moreover, an identity card, unlike a passport, is not primarily a travel document. It performs the function of a travel document only for travel between Member States, for entry into a Member State from a third country, and for exit into third countries with which agreements have been concluded under which an identity card can be accepted as a travel document. Although the recitals specify that identity cards have a predominantly internal function, it is also true that the genesis of the regulation can seemingly be explained by considering its function as a travel document. Recital 13 states that identity cards that are not travel documents do not fall within the scope of the regulation. The regulation on passports is the foundation on which Regulation 2019/1157 is clearly built. Biometric data does not seem to be so essential in enhancing the document's function of identifying the holder, if it is considered that States can continue to accept documents other than travel documents for proof of identity (recital 12), such as driving licences, which do not contain biometric data. Somewhat absurdly, a document that does not contain biometric data could be used to confirm the holder's identity in the event of a mismatch.

The purpose of Regulation 2019/1157 is then specifically identified. The objective, inherent in its legal basis, is to facilitate the free movement of persons. Recital 17 states that "[t]he inclusion of [...] biometric indicators [should] allow Union citizens to fully benefit from their rights of free movement". Given the importance of free movement of persons under EU law, this can easily be considered an ob-

---

41 Doubts are raised as to the appropriateness of the legal basis, although without going into the reasons, in Quintel, T., *The Commission Proposal and EDPS Opinion 7/2018 on the Proposed Regulation concerning Identity Cards and Other Documents*, European Data Protection Law Review, Vol. 4, No. 4, 2018, p. 510.

42 Articles 1 and 2 of Protocol (No. 22) on the position of Denmark. Articles 1 and 2 of Protocol (No. 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice.

43 The ordinary legislative procedure is considered more democratic and abstractly more preferable. However, it is settled case-law that the choice of procedure does not guide the choice of legal basis, but rather it is the legal basis that determines the procedure to be followed.

jective of general interest of the Union. Therefore, it is the necessity and proportionality of the collection and storage of biometric data that requires explanation.

The recitals to the Regulation state that identity cards and residence cards are among the most frequently falsified documents. This is not surprising, given the importance of proving one's status as a beneficiary of the right of free movement. Directive 2004/38 indirectly legitimises measures to combat falsification by allowing States to sanction the use of counterfeit documents by refusing the rights of residence applied for or by revoking rights previously granted. The point is to understand how the enhanced security of identity cards resulting from the inclusion of biometric data facilitates free movement. The explanatory memorandum accompanying the Commission's proposal contains a number of provisions, not included in the final regulation, which are enlightening: "secure identity cards and residence documents are essential elements to ensure the trust needed for free movement within an area of freedom and security" and "citizens can [...] not rely on their documents to exercise their rights if they cannot be sure that their documents will be accepted outside their Member State(s) of issuance". This assertion does not however appear to be supported by substantial evidence. True, there is anecdotal evidence of identity cards not being accepted and of a number of EU citizens experiencing difficulties when dealing with the public administration or with private parties because of identity cards not being accepted as proof of citizenship. But it does not seem immediately apparent that these difficulties are indicative of a structural problem requiring legislative intervention on a scale similar to that which happened for Regulation 2019/1157. Indeed, it would be possible to envisage a uniform model of identity card with advanced security features even without two types of biometric data.

Including biometric data in identity documents could facilitate free movement if it served to avoid or minimise the checks to which Union citizens would otherwise be subject. However, no proof of this is given.

Therefore, it does not appear that the regulation in question is pursuing an objective of general interest, considering its legal basis, such as to justify the limitation of fundamental rights arising from the taking and storage of fingerprints in identity cards. But even in the event that the proposed interpretation were not considered acceptable and that the objective pursued (whatever it may be) were considered one of general interest, the proportionality and necessity test would have to include, unlike what happened in *Schwarz*, an additional factor, namely the huge number of persons involved (all citizens of States where identity cards are compulsory, plus citizens of States where identity cards are not compulsory, if they apply for one) and the variety of circumstances in which an identity card must be

presented. In this context, false negatives or positives are likely to be particularly substantial in absolute value and therefore deserving of proper attention.[44]

5.1.3. Residence cards

The comments made in the previous section also apply to the legitimacy of collecting and storing biometric data in residence cards, albeit that a number of clarifications are required. Firstly, a residence card is neither an identity document nor a travel document. However, possession of a residence card exempts the holder from the requirement to hold a visa to enter a Member State from another Member State or from a third country. This function is to do with immigration management and prevention and control of unlawful immigration, with the result that the objective of general interest pursued with biometric passports can plausibly be extended to residence cards. However, the choice of Article 21(2) as the proper legal basis is debatable.

5.2. Storage and processing of biometric data for identification purposes

In *Schwarz*, the appellant then feared a further risk, which would have invalidated Regulation 2252/2004, namely the storage, centrally, of fingerprints collected in accordance with the Regulation and the use thereof for purposes other than authorised purposes. The Court acknowledges the existence of the risk, which is inherent in the use of fingerprints to identify persons, but considers this unfounded in this particular case, because the Regulation legitimises only the storage of fingerprints in the document, which remains in the holder's possession. Moreover, the Regulation cannot be interpreted as justifying the central storage of data or the use of such data for other purposes (paragraph 61). Once again, an important amendment is made by Regulation 444/2009, which adds a recital containing this principle and which is considered by the Court to be an interpretative principle that limits - or rather prevents - any extensive interpretation of the Regulation.

The Court returns to the subject of central storage and use of fingerprints in its judgment in the subsequent *Willems* case.[45] The case in question raises similar questions to those in *Schwarz*. The referring court asked the Court of Justice to interpret the Regulation as opposed to considering its validity. Of interest here is the Court's answer to the referring court's question on the interpretation of the Regulation as a basis for legitimising the storage of fingerprints in national databases. The national court asks whether Regulation 2252/2004, read in the light

[44] Quintel, T., *op. cit.* note 41, also highlights the increased risk of lost or stolen documents, p. 511.

[45] Joined Cases C-446/12 to C-449/12 [2015] ECLI:EU:C:2015:238.

of the Charter of Fundamental Rights, "must be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents." (paragraph 43). The Court reiterates the principle previously expressed in *Schwarz*, and takes it to its logical conclusion: the Regulation does not authorise the central storage of data or its subsequent use, but neither does it prohibit it. The Charter of Fundamental Rights is therefore the benchmark for assessing the legitimacy of States' conduct only if they act within the scope of EU law, which does not apply in the case in question. But the Court adds a rather frequent *obiter dictum*, acting *ultra petitum* and *ultra vires*, insofar as it does not look at the law which it is competent to interpret, but points out the obvious, not such much to the national court, because the question is hypothetical, as to all national legislative, administrative and judicial authorities: any State decision regarding the central storage or subsequent use of data would not escape judicial review by the national courts, to be conducted in the light of national law and, if appropriate, of the ECHR (paragraph 51). The Court does not examine the question in the light of Directive 95/46, which was in force at the time, because the referring court did not request an interpretation of that Directive.

The Court of Justice has made it abundantly clear that the regulations cannot justify a different use of the data. Regulation 2019/1157 is more explicit than Regulation 2252/2004 and requires the destruction of fingerprints once the document is handed over to the holder, but adds the sentence "Other than where required for the purpose of processing in accordance with Union and national law" (Article 10(3)).

Therefore, whether the Union or the Member States can use the data collected for other purposes is a question that cannot be resolved on the basis of the regulations relating to biometric documents. Given that States will be collecting a huge amount of photos and fingerprints, namely those of all their citizens (in States where the possession of an identity card is compulsory and of passport holders in States where it is not), it is not hard to imagine that States might also want to use them for other purposes (e.g. for police purposes or for preventing crime or fraud against State finances) and that question marks might be raised over that conduct.

The question of the legitimacy of the storage and processing of biometric data must therefore be addressed. Under EU law, biometric data is personal data if it is used to identify a person uniquely. The processing of such data is governed by three different Union acts: Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement

of such data;[46] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;[47] and Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.[48]

All of these acts define biometric data in the same way,[49] i.e. as personal data, the processing of which is governed by those acts, if it is processed in such a way as to allow or confirm the unique identification of a person. The rules on processing differ according to the purpose. For purposes relating to judicial cooperation in criminal matters and police cooperation, "the processing of [...] biometric data for the purpose of uniquely identifying a natural person" is possible "only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law" (Article 10 of Directive 2016/680). Article 76 of Regulation 2018/1725 is worded similarly: "Processing of [...] biometric data for the purpose of uniquely identifying a natural person [...] shall be allowed only where strictly necessary for operational purposes, within the mandate of the Union body, office or agency concerned and subject to appropriate safeguards for the rights and freedoms of the data subject". For different purposes, processing is prohibited, unless exceptions apply, including: "the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[50] According to Article 9(4) of Regulation 2016/679, Member States

---

46 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1.

47 Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L 119/89.

48 Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L 295/39.

49 Article 4(14) of Regulation 2016/679; Article 3(13) of Directive 2016/680; Article 3(18) of Regulation 2018/1725. For an analysis of Article 4(14) of Regulation 2016/69, see Jasserand, *op. cit*. note 18, as well as Bygrave, L.; Tosoni, L., *Article 4(14)*. *Biometric data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020.

50 Article 9(2)(g) of Regulation 2016/679. And also Article 10(2)(g) of Regulation 2018/1725.

may introduce further conditions including limitations. Where an exception applies, processing must still comply with the general conditions specified[51].

As legal scholars have highlighted, the processing of biometric data is regulated if it serves to identify the person, whereas processing for authentication or verification of a person's identity is not covered,[52] as this is an operation that is essentially carried out using the biometric data stored in identity documents.

Thus, analysing the relevant EU acts reinstates the possibility of collecting and processing biometric data for the purpose of uniquely identifying a person, albeit within strict limits to be carefully justified. On the other hand, it seems to exclude the possibility of interpreting these rules as prohibiting States or the Union from establishing such databases.

6. CONCLUDING REMARKS: DATABASES AND INTEROPERABILITY

The legitimacy of the collection and storage of biometric data, which the Court of Justice has addressed and resolved in its case law, should not be considered in isolation but rather placed within the broader debate on databases established by the Union or by Member States. On the one hand, it is evident that the databases established by the European Union have multiplied in number in recent years and many of them collect biometric data.[53] As legal scholars have pointed out, this is a form of cooperation between national authorities which is appreciated by States.[54] On the other hand, in more recent times, the Union has been pursuing the goal of

---

51 Article 6 of Regulation 2016/679, Article 5 of Regulation 2018/1725. Georgieva, L.; Kuner, C., *Article 9. Processing of special categories of personal data*, in: Kuner; Bygrave; Docksey; Drechsler (eds.), *op. cit.* note 49.

52 Bygrave, L.; Tosoni, L., *op. cit.* note 49.

53 EU databases are widespread in the area of immigration, where they are used to manage visa policy and international protection policy (EES, ETIAS, EURODAC, VIS) and in the area of police cooperation (ECRIS, SIS). Rijpma, J., *Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford University Press, Oxford, 2017, pp. 197 - 238.
Third-country nationals are now subject to a kind of mass data gathering. Indeed, records are kept of any third-country national entering the Union legally or illegally, whether they require a visa (VIS), do not require a visa (ETIAS or EES), are applying for international protection or are apprehended at external borders (EURODAC). There is plentiful discussion about whether such data gathering is lawful and whether it breaches the principle of non-discrimination on the basis of nationality, since EU citizens are not subject to the same measures. However, the discussion is following a strange course because instead of restricting data gathering in relation to third-country nationals, the trend is to intensify this in relation to Union citizens.

54 Brito Bastos, F.; Curtin, D.M., *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance*: *A Special Issue*, European Public Law, 2020, Vol. 26, No. 1, pp. 59 - 70, p. 60 et seq.

making databases interoperable, so as to make better use of the information they contain.[55] Interoperability connects different databases and makes the data stored in them searchable and accessible to a wider range of authorities and for different purposes from those for which the data is collected. A single search should be possible in all databases that the operator is authorised to access. So databases that are set up as independent and pursue a specific purpose (purpose limitation principle) may also be searched by different persons and for different purposes from those originally intended. Although this may be justified on the basis of the law, it represents a paradigm shift, which is more than the simple sum of its parts and cannot be considered legitimate simply because its individual components are legitimate. A change of this kind is a step towards widespread control that foreshadows a worrying society which, above all, is not the consequence of a conscious and democratically made political choice[56] but rather the collateral effect of administrative cooperation.

REFERENCES

BOOKS AND ARTICLES

1. Abeyratne, R.I.R., *The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject*, Annals of Air and Space Law, Vol. 17, Part 2, 1992, pp. 1 – 24
2. Baechler, S., *Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?*, European Journal on Criminal Police and Research, Vol. 26, 2020, pp. 379 – 394
3. Brito Bastos, F.; Curtin, D.M., *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance*: *A Special Issue*, European Public Law, Vol. 26, No. 1, 2020, pp. 59 – 70
4. Bygrave, L.; Tosoni, L., *Article 4(14)*, *Biometric data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020
5. De Coensel, S., *Terrorists on the move: a Legitimacy test of the Criminal Law approach on foreign fighters in Western Europe*, European Criminal Law Review, Vol. 10, No. 2, 2020, pp. 185 – 217
6. De Guttry, A.; Capone, F.; Paulussen, C., *Foreign fighters under international law and beyond*, T.M.C. Asser Press, The Hague, 2016

---

55 For an overview of the problems that interoperability poses, see the essays collected in the Special Issue cited in the previous footnote.

56 Gonçalves, M.E.; Gameiro, M.I., *Does the Centrality of Values in the Lisbon Treaty Promise More That It Can Actually Offer? EU Biometrics Policy as a Case Study*, European Law Journal, Vol. 20, No. 1, 2014, pp. 21 - 33 point out not only that biometric passports were adopted without discussion within civil society, but also that the decision to adopt them was motivated by the advantages to be gained from collecting biometric data, whereas the impact that this may have on individual freedom and democracy was not considered. Herting Randall, Hänni, *op. cit.*, note 16, at par. 18, point out that the establishment of central databases of biometric data "would undermine the symbolic value of the European Passport, turning it from a symbol of a common, right-based identity into a threat to civil liberties."

7. Georgieva, L.; Kuner, C., *Article 9. Processing of special categories of personal data*, in: Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020
8. Gonçalves, M.E.; Gameiro, M.I., *Does the Centrality of Values in the Lisbon Treaty Promise More That It Can Actually Offer? EU Biometrics Policy as a Case Study*, European Law Journal, Vol. 20, No. 1, 2014, pp. 21 - 33
9. Guild, E.; Peers, S.; Tomkin, J. (eds.), *The EU citizenship directive: a commentary*, Oxford University Press, Oxford, 2nd ed., 2019
10. Hagedorn, C., *Passport*, Max Planck Encyclopedia of Public International Law, 2008
11. Herting Randall, M.; Hänni, D., *European Passport*, Max Planck Encyclopedia of Public International Law, 2019
12. Hornung, G., *Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues*, European Public Law, Vol. 11, 2005, pp. 501 – 514
13. Jasserand, C., *Legal Nature of Biometric Data*: *From 'Generic' Personal Data to Sensitive Data*, European Data Protection Law Review, Vol. 2, No. 3, 2016, pp. 297 - 311
14. Lock, T., *Article 52 CFR*, in: Tomkin, J.; Klamert, M.; Kellerbauer, M. (eds.), EU Treaties and the Charter of Fundamental Rights: Digital Pack: A Commentary, Oxford University Press, Oxford, 2019
15. Quintel, T., *The Commission Proposal and EDPS Opinion 7/2018 on the Proposed Regulation concerning Identity Cards and Other Documents*, European Data Protection Law Review, Vol. 4, No. 4, 2018, pp. 505 – 514
16. Rijpma, J., *Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford University Press, Oxford, 2017, pp. 197 – 238
17. Torpey, J., *The invention of the passport: surveillance, citizenship, and the state*, Cambridge University Press, Cambridge, 2018

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-376/89 Giagounidis [1991] ECLI:EU:C:1991:99
2. Case C-459/99 MRAX [2002] ECLI:EU:C:2002:461
3. Case C-157/03 Commission v Spain [2005] ECLI:EU:C:2005:225
4. Case C-215/03 Oulane [2005] ECLI:EU:C:2005:95
5. Case C-291/12 Schwarz [2013] ECLI:EU:C:2013:670
6. Joined Cases C-446/12 to C-449/12 [2015] ECLI:EU:C:2015:238
7. Case C-101/13 U [2014] ECLI:EU:C:2014:2249
8. Case C-202/13 McCarthy [2014] ECLI:EU:C:2014:2459
9. Case C-246/17 Diallo [2018] ECLI:EU:C:2018:499
10. Case C-754/18 Ryanair Designated Activity Company [2020] ECLI:EU:C:2020:478
11. Case C-35/20 A [2021] ECLI:EU:C:2021:813
12. Case C-490/20 Stolichna obshtina, rayon 'Pancharevo' [2021] ECLI:EU:C:2021:1008

13. Case C-61/22 [2022] OJ C 213/22, Landeshauptstadt Wiesbaden, pending
14. Case C-280/22 Kinderrechtencoalitie Vlaanderen and Liga voor Mensenrechten [2022] OJ C 318/22, pending

EU LAW

1. Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals [2002] OJ L 157/1
2. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
4. Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77
5. Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L 119/89
6. Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2009] OJ L 142/1
7. Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1
8. Regulation 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders [2017] OJ L 74/1
9. Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L 295/39
10. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [2019] OJ L 188/67

UDK 366.542:004.738.5
Original scientific paper

TOUCH SCREEN JUSTICE AND CONSUMER VULNERABILITY – A MIXED BLESSING?*

Paula Poretti, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
pporetti@pravos.hr

ABSTRACT

Digitalization is the future and the future is now. New commercial possibilities in the digital market are constantly being explored and exploited. Phenomena such as ecommerce automation and the impact of big data use on transformation of retailer-consumer relationship are increasingly present and more familiar by the day. With them, new perspectives to render consumers vulnerable arise. The digital vulnerability, unlike other types of consumer vulnerability is a state typical of every consumer in the digital market. This notion challenges the existing consumer law and policy's ability to address the issues that arise in relation to such vulnerability with the traditional perspective. It also questions whether the redesign in the architecture of digital marketplaces is making the traditional architecture of dispute resolution obsolete. With these issues as a starting point, the paper assesses the current trend of streamlining consumer dispute resolution to AI tools and touch screen justice. We argue that under the current set up, instead of providing access to justice that is more available to consumers, this trend has a potential to generate a systemic vulnerability in itself.

Keywords: *access to justice, consumer, consumer vulnerability, digital market, dispute resolution*

1. DIGITALIZATION OF THE INTERNAL MARKET – THE RAISE OF THE DIGITAL MARKET

The fast pace of the technological progress allowed for a new dimension of the Internal market – the Digital market to become a reality of today's consumers. Online marketplaces offer more in terms of choice, convenience and even innovation in comparison to the classic retail shopping experience. With online shops virtu-

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ally transforming our smart devices into a department store or a high street allowing us to choose everything we could possibly need or want under our own roof and delivering it to us within days, it comes as no surprise that the Digital market is rapidly growing. As the recent survey of the Eurostat shows, online shopping is very popular in the EU and consumers appreciate the convenience of being able to shop anytime anywhere, having access to a broader range of products, comparing prices and sharing their opinion on goods with other consumers.[1] The proportion of individuals aged 16-74 having shopped online in the 12 months prior to the 2021 survey stood at 67 %. In the 12 months prior to the survey, 90 % of individuals aged 16 to 74 in the EU had used the internet, 74 % of whom had bought or ordered goods or services for private use. Online purchases by internet users increased by 20 percentage points compared with 2011.[2] However, due to the new commercial possibilities in the digital market, which are constantly being explored and exploited, phenomena such as ecommerce automation and the impact of big data use on transformation of retailer-consumer relationship are increasingly present and more familiar by the day. These practices aim at making consumers receptive to digital marketing strategies that use digital technologies to optimize commercial practices which can enhance the consumer experience, help the consumer to find the goods and services they are looking for, and intensify and personalize the relationship between trader and consumer. However, they can also be the source of new power imbalances between consumers and traders, and new forms of unfair commercial practices.[3] Hence, navigating the complex environment which the technology constantly redesigns and reshapes makes the relationships between consumers and traders challenging and requires consumers to acquire new knowledge and adapt to this swift-paced, evolving systems. In this sense, the search for means of empowering and protecting consumers in this new marketplace must go beyond the borders of already established framework of consumer protection under EU law. We argue that traditional understanding of the consumer should be reassessed in order to ensure that consumers are afforded a comparable level of protection *online* as they are *offline*. The New consumer agenda[4] (hereinafter: the Agenda) recognizes that the practices that accompanied the digitization of consumer markets disregard consumers' right to make an informed

---

1 Eurostat, *E-commerce statistics for individuals*, [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals#General_overview], Accessed 18 January 2023.

2 *Ibid.*

3 Helberger, N.; Sax, M.; Strycharz, J.; Micklitz, H.-W., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability Consumer vulnerability*, Journal of Consumer Policy, 45, 2022, p. 176.

4 Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM/2020/696 final.

choice, abuse their behavioural biases and distort their decision-making processes. Although the Agenda suggests that such practices would require additional guidance on the applicability of consumer law instruments such as the Unfair Commercial Practices Directive[5] (hereinafter: UCPD) and Consumer Rights Directive[6] (hereinafter: CRD), it offers no explicit mention on the scope or content of such interventions.

Hence, the paper challenges the existing notion of consumer and vulnerable consumer under the relevant consumer law and policy and its ability to address the issues that arise in relation to digital market practices. It also questions whether the redesign in the architecture of digital marketplaces is making the traditional architecture of dispute resolution obsolete. With these issues as a starting point, the paper assesses the current trend of streamlining consumer dispute resolution to AI tools and touch screen justice.

2. THE NOTION OF CONSUMER AND CONSUMER VULNERABILITY IN THE LIGHT OF DIGITAL TRANSFORMATION

The infrastructure of consumer protection in both EU consumer protection legislation and CJEU case law has been built upon the notion of consumer as reasonably well-informed and reasonably observant and circumspect, that is - an average consumer (Recital 18 UCPD). It starts from the presumption that a consumer who is well informed makes rational and reasonable decisions at the market, with no social or emotional influence.[7] This approach was criticized repeatedly already from the perspective of the traditional market functioning[8],

---

5 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L 149, pp. 22–39.

6 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance [2011] OJ L 304, pp. 64–88.

7 Incardona, R.; Poncibo, C., *The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution*, Journal of Consumer Policy Issue, Vol. 30, No. 1, 2007, pp. 21-38, pp. 31–36. See also Szilágyi, D., A *Challenge for the EU's Average Consumer Concept*, MTA–DE Public Service Research Group, 2020, [https://publicgoods.eu/challenge-eus-average-consumer-concept#_ftn11], Accessed 20 January 2023.

8 See Mišćenić, E., *Protection of consumers on the eu digital single market: virtual or real one?,* in: Viglianisi Ferraro, A.; Jagielska, M.; Selucká, M. (eds.), The influence of the European legislation on national legal systems in the field of consumer protection, Wolters Kluwer, 2018, p. 224.

but in the context of the digital market, it seems obsolete. Namely, digital consumer markets and electronic transactions use personalized persuasion strategies that discover, and build on emotions, biases, weaknesses and preferences of consumers precisely in order to affect their ability to make decisions rationally.[9] In this sense, both the notion of the average consumer and with it, the connected notion of the vulnerable consumer, need revisiting. Namely, these notions form together a benchmark from which commercial practices are assessed as accommodating for protecting users as the weaker party in commercial dealings and enabling consumers to play their role as active and autonomous market participants.[10]

When conceptualizing the new approach towards the understanding of the average and vulnerable consumer, the legal literature starts from the idea that the vulnerable consumer is no longer the exception, nor is the ordinary or average consumer the rule.[11] Quite the contrary, it seems that the digitalization of consumer market is making vulnerability a universal characteristic inherent to all consumers. In this sense, it seems appropriate to start from the changes in the understanding of consumer vulnerability and then circle back to the effect it had on the growing demands for changes in the existing definitions of average and vulnerable consumer.[12]

According to Article 5 para 3 UCPD vulnerable consumers are defined as: (i) a clearly identifiable group, (ii) vulnerable because of mental or physical infirmity, age or credulity, and (iii) a trader can be reasonably expected to 'foresee their vulnerability'.

The narrow approach towards defining vulnerability of consumers, as seen from the definition offered in the UCPD, clearly does not take into account the fact that vulnerability takes on different forms, depending on the situations or circumstances in which consumers find themselves. This is obvious from the results of the European Commission's 2018 consumer survey according to which 43 % of EU citizens believed themselves to be vulnerable as consumers. Digitalization of the market, with increase in the use of e-commerce and artificial intelligence is seen as one of the main triggers for making all consumers potentially vulnerable.[13] In this

---

9 Helberger; Sax; Strycharz; Micklitz, *op. cit.*, note 3, p. 180.

10 *Ibid.,* p. 178.

11 *Ibid*., p. 180.

12 See the Vulnerable consumers, Briefing, European Parliament, 2021.; Helberger; Sax; Strycharz; Micklitz, *op. cit.*, note 3, p. 182.

13 *"Dark patterns" and the EU consumer law acquis*, *Recommendations for better enforcement and reform surveys and submissions*, BEUC, Brussels, 2022, p. 4.

sense, a wider notion of consumer vulnerability should have, among other, a potential to embrace all dimensions of so-called 'permanent vulnerability' or 'vulnerability by default'[14] created by the architecture built on constant monitoring and manipulation of consumer behaviour and choices and exploitation of occurred or created vulnerabilities.

Building on this paradigm shift in understanding of who a consumer is and what constitutes a benchmark from which the unfair practice should be assessed within a changing digital market, the notion of the average consumer that describes the individual consumer is also in need of rethinking. The legal theory suggests a reversal of the positions in the relationship between the average and the vulnerable consumer. In this sense, it substitutes the reality of an average consumer - as an individual consumer - a relevant market player driven by information and choice, with a (dispositionally) vulnerable consumer.[15]

However, such a shift indicates a structural change in our perspective on the private law relationship between the consumer and the trader at the market. It also suggests that EU private law rules on consumer protection that governed that relationship cannot be transferred unambiguously to the digital market. Namely, the concept of consumer protection in the EU relied for the most part on the inherent tension between protecting users as the weaker party in commercial dealings and enabling consumers to play their role as active and autonomous market participants.[16] Nevertheless, with the use of AI and digital tools that predict what we are willing to pay for a product and streamline our choices towards it, consumers become essentially powerless and become vulnerable.[17] This erodes the role of (average) consumers who are now essentially vulnerable as active or autonomous participants in the market. Even more so, it distorts the very idea of regulated private autonomy as a tool necessary for supporting market integration.

The transformation of the consumer-trader relationship through digitalization and mainstreaming consumer vulnerability brings to the forefront the need to

---

14 *Regulating AI to protect the consumer*, *Position Paper on the AI Act*, BEUC, Brussels, 2021, pp. 22-23.

15 Helberger; Sax; Strycharz; Micklitz, *op. cit.*, note 3, p. 185.

16 *Ibid.*, p. 178.

17 An inclusive approach would require making vulnerability a core value of consumer protection policies and regulatory reforms rather than an afterthought as is currently the case. It requires a change of direction in the way consumer law has so far been created, away from neo-liberal economic concepts and the realisation of the internal market at EU level, to turn towards social concerns and protection. It is therefore regrettable that the only direct mention of 'vulnerable consumers' in the New deal appears with a commitment from the Commission to continue its efforts in consumer education. Riefa, C.; Saintier, S., *In search of (access to) justice for vulnerable consumers*, in: Riefa, C.; Saintier, S. (eds.), Vulnerable consumers and the law, Routledge, New York, 2021, p. 247.

discuss the adequacy of other elements essential for the functioning of the internal market. As one of these elements is administration of justice in consumer disputes, the perspective of its redesign will be discussed in the next chapter.

3. DIGITALIZED OR 'TOUCH SCREEN' JUSTICE

There are two alternatives available to Member States for providing access to justice to consumers, by way of private and public enforcement. On the private side, the possibility to resort to court or ADR entity existed long before the challenges to provide consumers substantive justice in case of infringements in the digital marketplace occurred. Moreover, pathways to private enforcement were developed without or with very little notion of practices that traders may employ in order to create digital asymmetries, which affect the decision-making autonomy of consumers. Even then, the possibilities for consumers to realize their rights before court or ADR entity were not without obstacles and limitations. As the legal literature rightly points out, they turn out to be insufficient and inappropriate to provide an adequate protection to the consumers, especially in situation of increasing number of cross-border breaches of consumer law.

Approaching the problem of providing justice to potentially vulnerable consumers in the digital era, by relying on the same procedural mechanisms and a slightly adjusted substantive framework, as suggested in latest EU consumer policy document, is rightfully criticised. In this sense, the central issue that should be discussed is the choice of mechanisms appropriate to provide justice to vulnerable consumers in a dispute arising from digital commercial practices.

3.1. Before ADR entities?

The traditional approach to providing access to justice to consumers starts from the basic private law principle of freedom of contract. Available private law mechanisms are put in place to ensure that courts or other competent authorities (such as ADR) provide remedy in case of an infringement of rights and obligations, arising out of the private law relationship entered into by consumer with a trader. Until now, both policy and implementing documents, whether on digitalization of justice[18] in the EU or enforcement of consumer protection[19] suggested that,

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalisation of justice in the European Union A toolbox of opportunities, COM(2020) 710 final.

[19] Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM/2020/696 final. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dis-

in terms of access, it is less complicated, more cost-effective, overall rational and natural to provide an online dispute resolution mechanism to consumers who have chosen to make online transactions. Such transfer of the dispute resolution forum for disputes arising online from the physical to the online environment seems as a rather straightforward, but also a quite mechanic response. Namely, from the perspective of universal consumer vulnerability this shift fails to take into account the problem that can be best decribed as "double digitalization" problem. The first part of this problem concerns the question, whether the characteristics of online dispute resolution mechanisms, which are advertised as facilitators of a more 'accessible' path to dispute resolution for consumers affected by digital commercial practices, hide the risk of exacerbating the existing vulnerability issues, due to the use of AI and digital tools. The second part of the problem concerns the very quality of the substantive justice delivered to consumers in such novel and complex disputes, not only by judges or ADR entities, but also by employment of algorithmic platforms and other similar smart solutions.

In order to assess the first problem, it is necessary to look at the accessibility of existing models of online justice for vulnerable consumers. Taking the online route in order to resolve a dispute for an EU consumer may mean that he will be approaching the online platform for alternative dispute resolution (hereinafter: ODR platform) put in place to offer a contact point which connects him with the traders who accept alternative dispute resolution (hereinafter: ADR).[20] The idea of introducing an ODR platform was again, mainly driven by the aim of supporting the single market and with no particular consumer vulnerability in mind. Its construction did not start from the presumption of potential vulnerability inherent to all consumers when exposed to the digital tools or content. It was focused en-

pute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) [2013] OJ L 165, pp. 63–79, Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [2013] OJ L 165, pp. 1–12.

[20] The platform itself has been developed as an interactive and multilingual webinterface offering a single point of entry to consumers and traders seeking to resolve disputes arising from online transactions without going to court. The platform, which is free of charge, can only be used by consumers and traders who are based in an EU country (including Norway, Iceland or Liechtenstein) and only for purchases made online either domestically or cross-border. The platform is not a complaint-handling tool in itself but it facilitates the transfer of cases to relevant ADR bodies. The platform helps consumers to find a route to the available ADR entities by connecting them with alternative (i.e. out-of-court) dispute resolution bodies, which can deal with their disputes. In this sense, the ODR Platform functions as a directory of available ADR services depending upon the type of complaint being pursued via the platform. Sciallis, E., *ODR and access to justice for vulnerable consumers, The case of the EU ODR Platform*, in: Riefa, C.; Saintier, S. (eds.), *Vulnerable consumers and the law*, Routledge, New York, 2021, p. 182.

tirely on features, which cater for more procedural economy, in terms of allowing consumers to contact the trader and initiate dispute resolution online, instead of appearing before court.

When compared to the access to court, which implies a lawyer representation, court fees and physical presence in proceedings of uncertain duration and outcome, ODR seems as proportionately more accessible solution. However, this assumption neglects the universal vulnerability perspective of all consumers and the obvious difficulties that might arise due to their inability to navigate a complex digital platform. This was further intensified recently, when a multi-level authentication for accessing the platform was introduced. Its complexity is based described by the fact that there is an elaborate guide on how to authenticate via mobile phone, a smart phone or a safety key.[21] There are several additional issues concerning accessibility. It is not uncommon for the consumers to confuse the link for accessing the platform that is displayed at the webpage of the trader with the trader's customer service. In terms of clarity of the information on the ODR platform, there is a system of self-help tabs, which are only accessible as a user progresses through the process. In addition, legal theory warns of several other issues, such as cross-platform support, accessibility for the disabled and interoperability with interfaces, especially for those using specialist keyboards or audio and reading aids that may create barriers in access.[22] It goes on to conclude that such a system cannot be considered as supportive enough for all users, especially the vulnerable ones.

In this sense, potential complexity of language, inaccessible pages for all insufficiently digitally literate or with disabilities, availability of different formats and presentations of communication and minutes of the meetings impair the available mechanisms in providing justice to vulnerable consumers.

The interface of the platform requires the consumer to present in detail all facts relevant for the dispute, including evidence. This can be confusing, as it does not suggest that the platform is a pre-access point for subsequent initiation of dispute before an ADR entity, which in the end might not even occur. All of the above can have a dissuasive effect for the average consumer. For a vulnerable consumer, depending on their type of vulnerability, it would be more likely for him to give up pursuing his claim all together.

---

21 For more on the Platform see European Commission, *Online Dispute Resolution*, [https://ec.europa.eu/consumers/odr/main/?event=main.home.selfTest], Accessed 25 January 2023. See the Guide at *EU Login*, European Commission, [https://webgate.ec.europa.eu/cas/manuals/EU_Login_Tutorial.pdf], Accessed 25 January 2023.

22 Sciallis, *op. cit.*, note 20, pp. 189-191.

Moreover, cases are recorded where traders used digital tools to discourage consumer from resolving the dispute before an ADR entity. However, legal theory warns that by renouncing the protection available through ADR mechanisms, consumers no longer have access to the record of their interactions with a trader, recorded in an accessible and transparent way either on the ODR platform or on the ADR systems.[23] This further complicates and prolongs the process of obtaining redress for vulnerable consumers and pushes them towards court proceedings as the only available, but hardly attainable recourse in practice.

The ODR system is obviously not equipped with solutions that recognize the problems of vulnerable consumers accessing and navigating the online site, understanding the online forms necessary to initiate procedures or participating in online proceedings without the assistance of lawyers. It is thus apparent that instead of facilitating access to justice to vulnerable consumers, the ODR can even add an additional layer of vulnerability and intensify the existing distrust in the system, in a moment when they need it most. This clearly highlights a need for revision of the ODR process in the light of a new understanding of roles and position of the various parties involved.

However, the major concern in connection to available national solutions on ADR connected to the ODR platform should be the fact that some of the mechanisms offered through the platform are actually offline (analogue) mechanisms that require the presence of parties. Unlike other characteristics of ODR discussed here, this one in fact undermines the idea of the ODR platform as a provider of online dispute resolution routes for consumers.

The procedural issues that touch upon "digitalized" justice, concern the appropriateness of using digital tools to resolve consumer, especially vulnerable consumer disputes, online. A separate issue is the quality of substantive justice that is delivered to consumers by relying on AI. The current development of ODR in EU, as explained, does not imply adjudication via the ODR platform. The ODR platform is merely a contact point that connects parties to the dispute and an ADR entity competent to resolve it. However, since the available legal tech tools could be used in future to digitalize the ADR mechanisms to which the ODR platform streamlines the consumer - trader disputes, it would be useful to try to project the potential advantages and disadvantages of such interventions for protection of universaly vulnerable consumers. The mechanisms that inspired the solutions examined further are already applied around the world.

[23] Sciallis, *op. cit.*, note 20, p. 190.

The application of legal tech arguably opens up the possibility for flexibilization and simplification of dispute resolution provided to consumers by way of ADR mechanisms. The use of AI, smart contracts and blockchain is particularly convenient in case of consecutive, systemic infringements, because they allow categorisation and use of smart patterns, as in the case of miscalculated utility bills. Although it might appear that the use of algorithmic assessment, which substitutes active participation of parties to the dispute, transforms ADR mechanisms into an even more accessible, effective, and less expensive means of providing access to justice to consumers, in reality there are issues concerning the use of AI in ADR that should not be overseen.

The use of smart patterns and systemic algorithmic solutions do not provide for a protective mechanism in terms of a virtual advisor who would help consumers, if they fail to understand the course of the procedure or have trouble navigating it. The mechanisms that rely on AI therefore often preselect only disputes that can be resolved by applying automated processes. Consumer whose disputes cannot be categorized as such are denied access.

Due to the use of sophisticated solutions, the technical legal vocabulary and online environment may cause consumers, especially the vulnerable to seek legal assistance, which is actually contrary to the idea of ADR as a dispute resolution without the participation of lawyers. Even the lawyers' assistance might still be of very limited effect, since they are not proficient in representing parties before advanced algorithmic systems as providers of AI-led ODR. Namely, their knowledge and skill in applying traditional procedural rules, including the rules on service of documents, taking of evidence or delivery of decisions might not be useful at all in such disputes.

Another issue arises in connection to the suitability of the consumer legislation for machine interpretation and application by AI, because the contemporary consumer law does not consist of precise and straightforward rules. There is also a question whether the AI is capable of understanding the limitations and vulnerability of consumers, which might have influenced their decision making-process. Namely, flexibility in the approach of rendering a decision that separates ADR from judicial procedure is not a given with AI-based ODR. Will AI be intelligible to the sensibility and skills acquired by legal practitioners in order to be able to recognize the readiness of parties to settle their dispute amicably? Or will the uniformity, speed and efficiency be sole considerations, which might ultimately result in developing a system that instead of facilitating, might be actually creating obstacles that exacerbate the problem of access to justice for the less affluent? Is in terms of ensuring the quality of provided justice to consumers the AI-based ODR system

able to produce decisions that will be recognized under national law of Member States? Obviously, many issues need unambiguous and unequivocal answers in order to assert whether AI is beneficial or detrimental to enhancing access to justice for universally vulnerable consumers of today's market.

3.2. Before court?

According to CEPEJ report from 2022, there are several significant and noticeable tendencies in the European judicial area, such as decrease in the number of courts, specialization in certain fields of law and a more pronounced reliance on ADR and the increased use of legal tech in the working processes of judiciary.[24] The common denominators to all of them, according to CEPEJ is the pursuit to foster the quality of justice. However, from the perspective of providing consumer protection, especially to the vulnerable, the tendency to consolidate courts might influence the accessibility of justice, regardless how high quality it strives to be. In addition, streamlining consumers from judicial procedures towards ODR, as manifested, may actually result in systemic creation of new forms of consumer vulnerability. The accelerated trend of digitalization of judiciary should also be reconsidered in this context. Since digitalization of ADR is obviously not without issues, it is interesting to try to examine whether in regard to court procedure it could hide a different potential.

The *New consumer agenda*, among other, emphasized that the revised legal framework for consumer protection consisting of a Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules[25] (hereinafter: Directive on better enforcement and modernisation of Union consumer protection rules) and Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC[26] (hereinafter: RAD) should substantially strengthen consumer rights, in particular by providing for

[24] *European judicial systems - CEPEJ Evaluation report - 2022 Evaluation cycle*, Council of Europe, 2022.

[25] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/ 83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328, pp. 7–28.

[26] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409, pp. 1–27.

more digital fairness, stronger sanctions and an effective mechanism for collective redress.[27] It is evident that regardless of facilitating individual protection being a priority at EU level, which is aimed to be achieved by modernising ECCs, ADR mechanisms and online dispute resolution, court procedures as still considered as the primary path to achieving consumer protection. Unlike digitalization of ADR, in the context of influence of digitalization on court procedure the debate is focused much more on building capacities for achieving a certain level of quality of provided justice. However, it seems that the efforts are mostly revolving aroung revising the substantive consumer law in order to disable traders to use advance technology to consumer detriment.

The Directive on better enforcement and modernisation of Union consumer protection rules provides measures such as an online entry point to be developed by the Commission should, as far as possible, be user-friendly, mobile-responsive, easily accessible and usable by all, including persons with disabilities ('design for all')[28] to be introduced in order to enhance ODR. In regard to judicial procedures, however it detects the remaining gaps in national law regarding truly effective and proportionate penalties to deter and sanction intra-Union infringements, insufficient individual remedies for consumers harmed by breaches of national legislation transposing Directive 2005/29/EC of the European Parliament and of the Council and shortcomings with regard to the injunction procedure under Directive 2009/22/EC of the European Parliament and of the Council, which the revised rules aim to eliminate. Revision of the injunction procedure is suggested to be addressed by a separate instrument amending and replacing Directive 2009/22/EC, which was achieved with the introduction of the RAD.[29]

However, the question of the intensified influence of digital technologies on delivering justice before court and the effect it might have on building or deteriorating the capacities of courts to apply the novel and complex legal concepts introduced within the substantive legal framework remains open. It is not clear if the digi-

---

27 Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM/2020/696 final, p. 15.

28 Recital 58 Preambule of the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1 [2019] OJ L 328, pp. 7–28.

29 Recital 3 Preambule of the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1 [2019] OJ L 328, p. 7–28.

talized judicial proceedings are adequately equipped to subordinate technology to the principles of justice. Will the principles of oral and public hearings be upheld? Is there a capacity for ensuring that the taking of evidence complies with the standards of a fair trial? Finally, will digitalization eventually result in eliminating the current parallelism of digital and 'analogue' systems of access to justice?

The general requirements connected to digitalization of judiciary are the respect for fundamental rights, such as the right to protection of personal information, fair trial and an effective legal remedy, as well as the principles of proportionality and subsidiarity. The European legislator also addresses the needs of the vulnerable groups. Regardless of the enhanced accessability and affordability of digital technologies, there should be institutional, organisational and technical measures in place to provide the vulnerable groups, without the necessary means or digital skills, a complete access to justice. The potential of AI tools in collecting and processing of data used to resolve a dispute is undeniable, in terms of both simplifying and reducing the duration of the procedure. Nevertheless, care must be taken that because there is a built-in potential of lack of transparency or partiality in some AI tools, there is a risk of undermined guarantees of the right to access to the judge and the right to a fair trial (equality of arms and respect for the adversarial process).[30] The design of machine learning models could hide a grave risk of racial, ethnic, socio-economic, political and religious, or sexual orientation biases, which should be minimized. Special attention should be given to the quality of learning data and patterns, including their representativity and relevance in regard to the purpose and context of the specific AI tool. Lack of transparency of AI tools could be problematic, due to the requirements of the right to a fair trial, including the equality of arms concerning parties in a dispute, right to a reasoned decision and other principles. Appropriate safeguards should be put in place in order to guarantee the protection of fundamental rights, including the equal treatment and data protection and to ensure the responsible, human-centric development and use of AI tools where their use is in principle appropriate. Buliding on these findings, the European legislator finds that the final decision-making must remain a human-driven activity and decision. Only a judge can guarantee genuine respect for fundamental rights, balance conflicting interests and reflect the constant changes in society in the analysis of a case. At the same time, it leaves room for the application and influence of the AI, but at the same time warns that such influence should not

[30] These questions were presented in the European Ethical Charter of the Council of Europe on the use of AI in judicial systems. The Charter aslo contains guidelines on addressing the challenges and the use of AI technology in a manner that equally respects the rights of all parties included. See more Council of Europe, *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, [https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment], Accessed 1 February 2023.

be exercised when judges give an explanation of their decisions. The proficiency and training of judges on the use of AI tools should therefore be provided as a protective measure agains any potential misuse.[31]

Dispite the risks, it is obvious that the digitalization of justice is increasingly relying on the AI. Therefore, the question whether in the context of the universally vulnerable consumers there are appropriate safeguards that the AI will recognize situations in which digital technologies are used to single consumers out, to make them dispositionally vulnerable through the choice architecture and (ab)use the inherent vulnerabilities of consumers to make them take decisions that we would otherwise not have taken should be discussed.[32] Will the court procedure under the influence of AI be able to offer consumers the possibility to fight lock-ins and data monopolies and ensure abolishing of unfair practices in the digital market?[33] Another valid issue arises in connection to the cognitive influence and the inability of humans (both vulnerable consumers and legal practitioners) to understand and process information at the same level as their digital counterparts. Namely, the legal literature suggests, that it is more difficult for technologies to recognise the more subtle signs of vulnerability, meaning that without human intervention, many clients will be railroaded down a tech-centred path when this may not be wholly appropriate.[34] How will consumers provide evidence on their lack of actual consent because, either they failed to understand privacy notices, or they considered it time-consuming to read the terms or all the same, because they cannot actually influence any of them? Will it be possible to require that in the case of the trader passively participating in an online marketplace and benefiting from its algorithmic environment, the burden of argumentation is on the provider of this environment to prove that the digital asymmetry, if present, is not used to materially distort the decision-making autonomy of the consumer, as the legal literature suggests?[35] It should be borne in mind that all of these challenges to realizing digital access to court and the digitalized court procedure should be tackled by consumers who often either rely on digital assistance, because they lack the basic digital skills or digital confidence, or they do not poses a device or internet connection, which enables them such access.

---

31 COM(2020) 713 at p. 11. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalisation of justice in the European Union A toolbox of opportunities, COM(2020) 710 final.

32 Helberger; Sax; Strycharz; Micklitz, *op. cit.*, note 3, p. 185.

33 *Ibid.*, p. 196.

34 *Simplifying access to justice for vulnerable consumers*, The Association of Consumer Support Organisations (ACSO), 2021, p. 8.

35 Helberger; Sax; Strycharz; Micklitz, *op. cit.*, note 3, p. 178.

Another possible path that would ensure private enforcement and, at the same time, relieve individual vulnerable consumers of the need to confront the challenges just mentioned, especially in connection to the use of AI, is by way of collective redress. It is undisputable that consumers may mandate consumer organisations (or other civil society organisations where relevant) to represent them individually.[36] However, they tend not to. Although RAD enables consumers to use a representative action in order to defend their rights at least collectively, there is strong criticism against introducing such possibility. Some critics consider representative actions to be complex, due to multiple plaintiffs and quantifications of damages, and overburdensome for the consumers.[37] Others suggest that the AI Act[38] is not pure consumer protection legislation and therefore, the representative actions as offered in RAD, could not be used as mechanisms for protection of consumer rights under the Act.[39] This position fails to take into account that AI Act is one of the strategic consumer protection measures included in the Commission's Consumer Agenda of 2020.[40] Advocating for introduction of the AI Act to the RAD Annex I or the RAD in the proposal for an AI Act means requesting that consumer organsations are allowed to initiate a claim against illegal commercial practices or for obtaining compensation in case consumers suffered harm by a non-compliant AI system and its practice. It would also mean that the full effectiveness of the AI Act is not only envisaged, but also granted to consumers.[41]

4. CONCLUSION

Just as the digital market provides consumers with countless possibilities to enter trader – consumer relationships, that do not necessarily end with the purchase or delivery of the product or service, its architecture leaves ample room for using the existing and creating new consumer vulnerabilities to the benefit of the traders. Namely, the use of digital tools allows traders to influence consumer decisions profoundly, leaving them without actual autonomy in their decision-making process. This essentially puts all consumers in an equally vulnerable position, for some adding an additional layer to already existing situations of vulnerability. The

---

36 *Reasons to Add the AI Act to the Representative Actions Directive*, BEUC, Brussels, 2022.

37 *Ibid.,* p. 2.

38 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.

39 *Reasons to Add…op. cit.*, note 36, p. 3.

40 *Ibid*., p. 3.

41 Micklitz, H-W.; Helbergeri, N.; Rott, P., *The Regulatory Gap: Consumer Protection in the Digital Economy*, *Addendum to the report 'Structural asymmetries in digital consumer markets*, BEUC, Brussels, 2021, p. 23.

creation of such universal consumer vulnerability challenges the private autonomy regulated by way of consumer protection law, which the internal market relies on. However, it also gives rise to concerns whether the traditional *ex post* private law mechanisms of dispute resolution that perceive that autonomy as inherent to the relationships from which the disputes arise are sufficient and appropriate to enable access to justice to universally vulnerable consumers. The starting point of the efforts in digitalization of traditional dispute resolution mechanisms to date was the desire to speed up the dispute resolution procedures, facilitate the exchange of information and documents with parties and lawyers, and provide continuous and simple access to justice. This resulted in an increase in the use of information and communication technology (ICT) tools and the promotion of the use of secure and high-quality technology for remote communication (video conferencing). [42] However, the measures taken in the sphere of designing procedural mechanisms do not take into account that the influence of digitization results in a power imbalance between the transacting parties and allows procedural exploitation in contract law, which ultimately causes an erosion of private autonomy. In this sense, as the analysis of the observed mechanisms showed, they are often inappropriate and not adapted to the requirements on ensuring access to justice to universally vulnerable consumers, creating additional, systemic vulnerability.

In this sense, as the analysis of the observed mechanisms showed, they are often inappropriate and not adapted to the needs of ensuring access to justice to universally vulnerable consumers, creating additional, systemic vulnerability. This can even be partially attributed to the disparity between the goals of digital transformation policies aimed at improving the judiciary, on the one hand, and consumer protection, on the other. In this context, it is not negligible that the policy of consumer protection is increasingly growing, from a policy of technical harmonization of standards to support the internal market, into a vital part of efforts to advance the goal of establishing a "Europe of Citizens".[43] However, to the disappointment of many legal theorists, the relatively recent creation of a representative action and the adoption of the AI Act within the framework of consumer protection policy was not seen as an opportunity for an important step towards achieving that goal. In this sense, in the period ahead, it will be crucial to move away from the idea of digital transformation of administration of justice as merely an introduction of software and hardware solutions as main 'deliverers of justice'.

---

42 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalisation of justice in the European Union A toolbox of opportunities, COM(2020) 710 final.

43 See more European Parliament, *Consumer policy: principles and instruments*, [https://www.europarl.europa.eu/factsheets/hr/sheet/46/politika-zastite-potrosaca-nacela-i-instrumenti], Accessed 4 February 2023.

Improving routes to redress via access to dispute for universally vulnerable consumers requires a more coherent approach. The measures taken should be based on a profound understanding of each pattern of consumer law infringements at the digital market and the appropriateness of a specific mechanism for achieving policy objectives of consumer protection. Only this can be a guarantee that digital market practices, which create systemic vulnerability that erodes the private autonomy of EU citizens and has deeper societal implications will be removed from the market.

REFERENCES

BOOKS AND ARTICLES

1. Helberger, N.; Sax, M.; Strycharz, J.; Micklitz, H.-W., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability Consumer vulnerability*, Journal of Consumer Policy, 45, 2022, pp. 175-200
2. Incardona, R.; Poncibo, C., *The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution*, Journal of Consumer Policy Issue, Vol. 30, No. 1, 2007, pp. 21-38
3. Mišćenić, E., *Protection of consumers on the eu digital single market: virtual or real one?,* in: Viglianisi Ferraro, A.; Jagielska, M.; Selucká, M. (eds.), The influence of the European legislation on national legal systems in the field of consumer protection, Wolters Kluwer, 2018, pp. 219-246
4. Riefa, C.; Saintier, S., *In search of (access to) justice for vulnerable consumers*, in: Riefa, C.; Saintier, S. (eds.), Vulnerable consumers and the law, Routledge, New York, 2021, pp. 1-16
5. Sciallis, E., *ODR and access to justice for vulnerable consumers, The case of the EU ODR Platform*, in: Riefa, C.; Saintier, S. (eds.), Vulnerable consumers and the law, Routledge, New York, 2021, pp. 177-192

EU LAW

1. Communication from the Commission to the European Parliament and the Council, New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM/2020/696 final
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalisation of justice in the European Union A toolbox of opportunities, COM(2020) 710 final
3. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L 149

4. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance [2011] OJ L 304
5. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) [2013] OJ L 165
6. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/ 83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328
7. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409
8. 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.
9. Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [2013] OJ L 165
10. The Vulnerable consumers, Briefing, European Parliament, 2021

REPORTS

1. "*Dark patterns" and the EU consumer law acquis, Recommendations for better enforcement and reform surveys and submissions*, BEUC, Brussels, 2022
2. Micklitz, H-W.; Helbergeri, N.; Rott, P., *The Regulatory Gap: Consumer Protection in the Digital Economy*, *Addendum to the report 'Structural asymmetries in digital consumer markets*, BEUC, Brussels, 2021
3. *Reasons to Add the AI Act to the Representative Actions Directive*, BEUC, Brussels, 2022
4. *Regulating AI to protect the consumer*, *Position Paper on the AI Act*, BEUC, Brussels, 2021
5. *European judicial systems - CEPEJ Evaluation report - 2022 Evaluation cycle*, Council of Europe, 2022
6. *Simplifying access to justice for vulnerable consumers*, The Association of Consumer Support Organisations (ACSO), 2021

WEBSITE REFERENCES

1. Council of Europe, *European Ethical Charter on the use of AI in judicial systems*, [https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment], Accessed 1 February 2023

2. European Commission, *EU Login*, [https://webgate.ec.europa.eu/cas/manuals/EU_Login_Tutorial.pdf], Accessed 25 January 2023
3. European Commission, *Online Dispute Resolution*, [https://ec.europa.eu/consumers/odr/main/?event=main.home.selfTest], Accessed 25 January 2023
4. European Parliament, *Consumer policy: principles and instruments*, [https://www.europarl.europa.eu/factsheets/hr/sheet/46/politika-zastite-potrosaca-nacela-i-instrumenti], Accessed 4 February 2023
5. Eurostat, *E-commerce statistics for individuals*, [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals#General_overview], Accessed 18 January 2023
6. Szilágyi, D., *A Challenge for the EU's Average Consumer Concept,* MTA–DE Public Service Research Group, 2020, [https://publicgoods.eu/challenge-eus-average-consumer-concept#_ftn11], Accessed 20 January 2023

UDK 341.41:623.4]:004.8
Original scientific paper

RETHINKING COMMAND RESPONSIBILITY IN THE CONTEXT OF EMERGING AI WEAPONS*

Igor Vuletić, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
ivuletic@pravos.hr

ABSTRACT

This paper addresses the issue of command liability for severe criminal offenses committed by means of autonomous and semi-autonomous weapons. Research has shown that the leading military forces around the world are intensively working on designing autonomous weapons, which will provide them an enormous tactical ad logistical advantage in warfare. As the national and international law concept of command responsibility to date has been based on the idea of humans selecting and ordering the destruction of targets, the author raises the question of whether this has also created a set of legal norms that could adequately regulate such situations in the context of new warfare techniques. The first section of the paper briefly outlines the direction of the development of autonomous weapons. The second section analyzes the provisions on command responsibility of the Rome Statute and the Statute of the ad hoc tribunals for Yugoslavia and Rwanda. The national legislation of some countries and the significant jurisprudence in this field is also analyzed and projected into the context of semi-autonomous and autonomous warfare. A special emphasis is placed on the issue of unconscious negligence. The objective of the paper is to indicate the legal gaps and to propose guidelines for future development.

Keywords: *autonomous – weapons – commander – liability – punishment – negligence- causality - targeting*

1. INTRODUCTION

The development of artificial intelligence (AI) is one of the trends, which is likely to revolutionize various sectors. Artificial intelligence has permeated sectors such as medicine and the vehicle industry. However, this trend is particularly progres-

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

sive in the military industry, with many global military super powers defining the development of autonomous weapons as their strategic objective for the near future. This type of weapons is believed to have numerous advantages over the traditional types of weapons, including the reduction of human casualties for the users, higher level of precision and effectiveness as well as lower costs, etc.[1]

On the other hand, an increased level of automatization in this sector could also have potentially harmful effects and create legal dilemmas and/or loopholes, which cannot be adequately addressed within the existing legal framework.[2] For instance, would an automated system be able to distinguish between a terrorist and an ordinary hunter carrying a gun on his shoulder? In addition, would a commander be responsible in this scenario if the system selected and destroyed the wrong target? Such scenarios are not impossible, as some relatively recent cases demonstrate; e.g.in 1988 the American radar system „*Aegis*", whose purpose was protecting the battle ships from aerial attacks, confused an Iranian civilian airplane Iran Air 665 with a military aircraft and launched an antiaircraft rocket, causing the death of all 290 passengers and crew members.[3]

This paper seeks to contribute to the already existing discussion from two different angles. Firstly, we will assess the current level of automatization of the most highly developed military systems, as well as the plans for their future development. In this context particular attention will be devoted to the issues of both the existing and desired level of autonomy of the weapons in the detection and selection of targets, their methods of operation and the ability of humans to communicate with the weapons and order a last-minute recall. After establishing the measure in which the autonomy of the weapons also implies its genuine independent decision-making, we will then bring the discussion into the context of command liability in international criminal law. Special consideration will be given to the issues of causality and culpability (the foreseeability of the consequence), taking into account different interpretations, which exist on this matter in civil law and common law traditions.

The aim of this paper is to determine whether the gradual introduction of autonomous warfare into military operations also demands the modification (or fundamental alteration) of the existing concept of command responsibility.

---

1 Mauri, D., *Autonomous Weapons Systems and the Protection of Human Persons – An International Law Analysis*, Edward Elgar Publishing, Cheltenham – Northampton, 2022, p. 7.

2 For a discussion from the human rights perspective see *ibid*. See also e.g. Grut, C., *The challenge of autonomous lethal robotics to international humanitarian law*, Journal of Conflict and Security Law, Vol. 18, No. 1, 2013, pp. 5–23.

3 See more Simple Flying, *34 Years Ago Today: The Shootdown Of Iran Air Flight 655*, 2022, [https://simpleflying.com/iran-air-flight-655-1988-shootdown-anniversary/], Accessed 27 July 2022.

2. AUTONOMOUS WEAPONS: WHERE DO WE STAND?

In order to be able to competently discuss the issue of command responsibility for the acts of autonomous weapons, it is important first to clearly define the concept of autonomous weapons, although there is no consensus in this regard.[4] According to the British Ministry of Defense, in order for a weapon to be autonomous, it must be „*capable of understanding higher level intent and direction and take appropriate action to bring about the desired state*".[5] This definition, however, raises a considerably high requirement which is currently far from realization, and such autonomous weapons are conceivable only in the far future. Therefore, the following analysis will be based on a more pragmatic definition provided by the US Department of Defense, stating that any weapon with the capacity, when activated, independently „*select and engage targets without further human intervention*".[6] The latter definition covers weapon systems that are already developed today and are in possession of the most developed global military forces. Autonomous weapons should be distinguished from automatic weapons which are programmed in a way to follow a logical chain of rules without making independent decisions on the selection of the targets and the course of action.[7]

The first known instance of the use of autonomous weapons happened in the conflict between Azerbaijan and Armenia in Nagorno-Karabakh in 2016. The Azerbaijan military gained a significant tactical advantage by using advanced Israeli autonomous weapon IAI Harop loitering munition, also known as the „kamikaze drones."[8] This is a special type of rocket which, once launched, can hover in the air for hours and „lurk" over enemy targets before striking and destroying them, similar to the Japanese kamikazes in World War II.[9]

For the classification of autonomous weapon systems in this paper, we will adopt the one provided by the Stockholm Peace Research Institute (SIPRI) in line with the definition of the US Department of Defense. According to this classification, autonomous weapons can be divided into the five categories described in the following sections.[10]

---

4 Mauri, *op. cit,* note 1, p. 24.

5 UK Ministry of Defence, *Joint Doctrine Publication 0-30.2., Unmaned Aircraft Systems*, 2017, p. 13, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf], Accessed 28 July 2022.

6 US Department of Defense, *Directive No. 3000.09*, 2017, pp. 13-14, [https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf], Accessed 28 July 2022.

7 *Supra* note 5.

8 Postma, J., *Drones over Nagorno-Karabakh,* Atlantisch Perspectief , Vol. 45, No. 2, 2021, pp. 15 – 20.

9 See HAROP, *Loitering Munition System*, [https://www.iai.co.il/p/harop], Accessed 28 July 2022.

10 Boulanin, V.; Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems*, SIPRI, Solna, 2017, pp. 36 - 54,.

A) *Air defense systems*

These systems operate by discovering potential aerial threats through a radar, assessing the danger risk and independently determining whether to attack. The final decision on the course of action, thus, falls on the system. The human behind the system decides on its activation, oversees its operation and has the power to turn it off at any point.[11] There are multiple types of such air defense systems. Examples include the Dutch *GoalKeeper* and the US *Phalanax*, which are usually mounted on battle ships, or the German *MANTIS*, which serves for the protection of land army bases. It should be noted that such systems have been developed since World War II and that they are very sophisticated and effective nowadays.[12] In the past, air defense systems have cause numerous civil casualties, as in the case of the US *Aegis* system, which brought down an Iranian civilian airplane due to a wrong assessment, causing the death of 290 passengers.[13]

B) *Active protection systems*

The role of actuve protection systems is to protect armored vehicles from rocket attacks. The system is programmed to independently recognize and intercept certain projectiles. Examples include the Swedish- South African *LEDS-150* system, or the Israeli *Trophy.* These systems work under the same principle as the previously described air defense systems, which means they use radars for the detection of projectiles and a specially designed operational software. Such systems have been developed since the 1970s, and there are 17 registered autonomous weapons of this type to date.[14]

C) *Robotic sentry weapons*

Robotic sentry weapons are gun turrets which can independently detect and follow a target, and also shoot when needed. They can be used mounted on a vehicle and they can shoot from the ground when necessary. Unlike the previous two systems, they have been developed since the early 2000s, which is why there are only three known types. At the operational level, considering their development stage, they are mostly used for the surveillance of enemy movement.[15]

---

11 *Ibid.*, pp. 36 – 37.

12 *Ibid.,* p. 37.

13 *Supra* note 3.

14 Boulanin; Verbruggen*, op. cit.,* note 10, p. 41.

15 *Ibid.,* pp. 44 – 47.

D) *Guided munitions*

Guided munitions (also known as precision-guided munitions and smart bombs) do not fully satisfy the autonomy standards according to the US Department of Defense definition, because humans select their targets.[16] They are, nevertheless, included in this classification because of their ability to independently correct the initial targeting. Their autonomy, thus, relates only to the phase of the course of the projectile towards the target, after the target has been determined. This is why they were initially excluded from the SIPRI classification, but they were subsequently added because they provide an insight into the development of the autonomous targeting technology.[17]

E) *Loitering munitions*

Finally, loitering munitions, which have already been mentioned earlier in the context of the Nagorno-Karabakh conflict are a type of autonomous weapon with the capacity to fly over an area for a particular time and to „lurk" over the target before descending towards it in a manner comparable to the Japanese kamikaze from World War II. The only role of the humans in in this sense is to launch the projectile which then proceeds to operate fully autonomously. It is important to note that they are not assigned a concrete target in advance (it is chosen by them independently), but only the flyover area.[18] Here, the use of the drones in the war in Ukraine could also be mentioned as an example of such technology.[19]

The previous elaborations lead to the conclusion that the advent of autonomous weapons in the military industry is becoming more intensive. Because of the tactical advantages provided by the autonomous systems in combat, the leading global military forces are broadly accepting this type of weapons, regardless of the UN initiative to reduce or even eliminate the use of this type of weaponry.[20] The available reports do not allow a precise conclusion on the level of influence and control of the person behind the system. Namely, exact information about each of the existing systems, as well as those currently developed are treated as military

---

16 For more in this context see Amoroso, D., *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, Nomos, Napoli, 2020, p. 19.

17 Boulanin; Verbruggen*, op. cit.,* note 10, p. 47.

18 *Ibid.,* p. 50.

19 The Messenger, *The Ukraine War in data: Winning the drone war*, [https://www.grid.news/story/global/2023/01/05/the-ukraine-war-in-data-winning-the-drone-war/], Accessed 13 February 2023.

20 Gill, A. S., *The Role of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons,* UN Chronicle, Vol. 55, No. 4., 2019, pp. 15 – 17.

secrets and they are not publicly available. Experts in this area agree that human involvement is not always a guarantee of safe operations. To the contrary, it can present an additional danger if the operating person is not properly trained, or if the information input into the system is too complicated or insufficiently clear.[21] In this sense, literature indicates the difficulties in the determination of liability for severe offenses and violations of international humanitarian law committed by autonomous weapons.[22]

This issue can be observed primarily from the present perspective. Namely, although the management of military operations is still primarily a human task, there are at least thirty military forces around the world that function with significant reliance on so-called supervised autonomous weapons, which means that the system is in charge of targeting (search, identification, tracking and prioritization of targets), while the humans in the background make the final decision makes the final decision on the basis of such information.[23] These systems, also known as Automated Target Recognition (ATR), function under the principle of the so-called pattern recognition, which consists of the identification of military targets based on so-called target signatures, which are previously set by persons in the background.[24] If this mode of operations leads to the killing of civilians or the destruction of civilian targets, it opens complex issues of criminal law related to the predictability of the operations of the supervised autonomous system, or the so-called „many hands" problem[25] and the insufficient basis for an adequate level of liability. Literature warns of potential issue with the capacity of ATR-based system to accurately and precisely distinguish targets in accordance with the rules of international humanitarian law. This brings to light the inadequate level of field testing of the system as well as its over-fitting, and inability to program in light of the standards of international humanitarian law (since legal standards require human interpretation).[26]

On the other hand, this legal situation can also be observed from the prism of the (near) future, when it is likely that fully autonomous weapon systems will take the

---

21 *Ibid.,* p. 40.

22 United Nations Institute for Disarmament Research (UNIDIR), *Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies*, Geneva, 2016, p. 16, [https://unidir.org/publication/safety-unintentional-risk-and-accidents-weaponization-increasingly-autonomous], Accessed 28 July 2022.

23 Scharre, P., *Centaur Warfighting: The False Choice of Humans vs. Automation,* Temple International and Comparative Law Journal, Vol. 30, No. 1, 2016, p. 154.

24 Boulanin; Verbruggen, *op. cit.,* note 10, p. 25.

25 *Ibid.*, pp. 127 – 131.

26 *Ibid*., p. 25.

key role in the operational functioning on the battle field, and thereby also in key decision-making.[27] The related legal issues will become even more complicated since it will be much more difficult to construe legal liability of persons behind the weapon system. In addition, the insufficiently developed concept of criminal liability of legal entities at the international level will become even more complicated.

In the following sections we will turn to the criminal law dimension of the issue and we will address the question of whether the existing framework of command responsibility (at the national and supranational levels) is sufficient to encompass the potential situations of command responsibility if an autonomous system establishes the characteristics of an international criminal offense.[28]

3. SUPERIOR LIABILITY FOR AUTONOMOUS WEAPONS: RETHINKING THE SCOPE AND THE LIMITS

Command responsibility is one of the key institutes of international criminal law whose normative origins lay in the Hague Conventions. This concept was first applied during Leipzig process after World War I and it was affirmed in the trials for War World II crimes and the practice of the ad hoc courts for former Yugoslavia and Rwanda.[29] A turning point in the development of the concept of command responsibility was the judgment against the Japanese general Tomoyukij Yamashita for the crimes of his troops on the Philipines during World War II. This judgment established the legal standard for the liability of commanders for the crimes of their subordinates evennif they did not order such acts, but failed to undertake measure to prevent them.[30] Ever since then, and to this day, a significant body of case law has been built both by the international criminal tribunals, as well as the national courts of the countries in which war crime proceedings have been, or still are conducted.[31] A wealth of literature has also been dedicated to this issue. Nevertheless, it seems that the concept of command responsibility is still in its

---

27 See e.g. Matthias, A., *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata,* Ethics and Information Technology, Vol. 6, No. 3, 2004, pp. 175 - 183.

28 In literature, there is a lack of consensus on the definition and list of international crimes. In this paper, we are adopting *Bassiouni`s* definition of international crimes. See Bassiouni, M. C., *Introduction to International Criminal Law*, Second Revised Edition, Brill-Nijhof, Leiden, 2014, pp. 138.

29 Ching, A. B., *Evolution of the Command Responsibility Doctrine in Light of the Celebici Decision of the International Criminal Tribunal for the Former Yugoslavia,* North Carolina Journal of International Law, Vol. 25, No. 1, 1999, pp. 169 – 176. See also Martinez, J. S., *Understanding Mens Rea in Command Responsibility*, Journal of International Criminal Justice, Vol. 5, No. 3, 2007, pp. 647 – 660.

30 Ching*, op. cit.,* note 29*,* p. 181.

31 For example, in Croatian jurisprudence command liability is based on common principle of criminal responsibility for inaction. *See* e.g. Supreme Court of the Republic of Croatia*, Case No. Kž-rz 22/2018*.

development stage and that with each new case the courts face challenges which were not previously addressed. For example, *Martinez* rightfully warns that, even after a 50-year evolution of the doctrine of command responsibility, the issue of the scope of *mens rea* remains unclear.[32] On the other hand, *Bonafé* emphasises the issues related to the relatively small number of convictions based on command responsibility for typical military operations.[33]

The statutes of ad hoc tribunals, as well as the Rome Statute accept this standard but with the addition that he commander had acted with a certain type of *mens rea*, which means they knew or had reason to know of the acts of their subordinates. [34] The Rome Statute provides a much narrower liability of a civil commander than that of a military commander because the latter is also liable for unconscious negligence[35] (*should have known*), while civil commanders must be aware of all the circumstances and willfully disregard their duties.[36] It is worth noting that some national systems provide a much more lenient punishment for the negligent form of command responsibility, based on the essential difference between willful and negligent criminal offenses. Thus, such legal systems treat the negligent form as a special (less severe) criminal offense compared to the willful form of command responsibility. There are examples of such provisions in German and Croatian criminal law.[37] This regulatory regime is based on the principles of the criminal law dogmatic in continental Europe and it significantly differs from the approach in international criminal law, so it was often subjected to criticism.[38] We will not engage in a discussion of the merits of such a distinction because this would be outside of the scope of this paper.

From the practice of international and national courts to date has revealed that, in order for the commander to be liable under the established standards, several objective preconditions have to be met cumulatively: 1. The perpetrators of the specific criminal offense must be directly subordinated to the commander; 2. The commander must have an effective (real) ability to control ir subordinates; 3.

---

32 Martinez, *op. cit.,* note 29, p. 638.

33 Bonafé, B. I., *Finding a Proper Role for Command Responsibility*, Journal of International Criminal Justice, Vol. 5, No. 3, 2007, pp. 599 – 618.

34 See Rome Statute, Article 28; ICTY Statute, Article 7; ICTR Statute, Article 6.

35 Negligence as a form of guilt was sometimes denided in case law prior to the Rome Statute. See e.g. *Prosecutor vs. Bagilishema,* Appeals Chamber Judgement (ICTR), Case No. ICTR – 95 – 1A-A, 3 July 2002, para. 35.

36 Rome Statute, Article 28 (a) (i).

37 See German Völkerstrafgesetzbuch, Article 4; Croatian Criminal Code, Article 96.

38 As an example of criticism, see European Parliament, *European Parliament Resolution of 16 February 2011 on the 2010 progress report on Croatia*, para. 15, [https://www.europarl.europa.eu/doceo/document/TA-7-2011-0059_EN.pdf], Accessed 1 August 2022.

There must be a causal link between the criminal offense of the subordinates and the failure of the commander to exercise their effective control; 4. the commander must fail to undertake preventive measures that are necessary and could be reasonable expected in the specific situation. If the criminal offense was yet to be committed, the relevant measures would be of a preventive nature and otherwise the measures would be aimed at the processing and sanctioning the perpetrators.[39]

With regards to the subjective relationship with the offense (*mens rea*), a negligent commander should be familiar with the fact that their subordinates are preparing to commit an offense. This awareness of the facts creates certain controversies in theory and practice and it is difficult to prove at times. It can be stated in principle that negligence exists when the perpetrator is unaware of the facts underlying the criminal offense, but could or should be aware of them, under the standard of due care expected from them. [40] Thus, negligence is a violation of the duty of due care, with the cumulative violation of objective due care (that expected from any average person) and subjective care (which is expected from a particular perpetrator).[41]

The determination of such *mens rea* for command responsibility has proven to be very difficult in practice. Firstly, there are significant differences in the understanding of negligence in civil law and common law jurisdictions. In some common law countries, there are different interpretations of the duty of care standard. For example, some common law countries distinguish ordinary, gross and criminal negligence, while others do not.[42] On the other hand, civil law systems use a completely different terminology and they distinguish *dolus* (intent) from *culpa* (negligence), both of which branch out into sub-categories. The unharmonized terminology related to the liability is probably most pronounced in relation to *dolus eventualis* because this term can be subsumed under both recklessness and intent.[43] This is why there have already been attempts in literature to find a harmonized categorization of the types of liability, which would be applicable in all systems.[44] The analysis of certain cases related to command responsibility before national courts shows how liability for negligence can be excluded and the inter-

---

39 Satzger, H., *International and European Criminal Law,* C. H. Beck – Hart – Nomos, München – Oxford, 2012., p. 242.

40 See e.g. American Law Institute, Model Penal Code (1962), at 2.02(2)(d).

41 See e.g. Jescheck, H.-H.; Weigend, T., *Lehrbuch des Strafrechts. Allgemeiner Teil,* Duncker & Humblot, Berlin, 1996, pp. 577 - 582.

42 See more in Martinez, *op. cit.,* note 29, p. 644.

43 *Ibid.,* pp. 644 – 645.

44 Blomsma, J., *Fault elements in EU criminal law: the case for recklessness*, in: Klip, A. (ed.), Substantive Criminal Law of the European Union, Maklu, Antwerpen, 2011, pp. 139 – 159.

pretations that only *dolus eventualis* is possible.[45] However, this type of liability is interpreted somewhat more broadly, taking into account whether the commander took into account the profiles of the (subordinated) perpetrators during the formation of the troops, taking into account their level of education prior experience, past life and possible revenge motivations (for example, whether members of their families were killed in the war=the risk of the presence of possible victims in a particular area, the clarity of thein light of international humanitarian law, etc.[46] This indirectly establishes a legal standard comparable to the violation of due care as the basis for (civil law) negligence.

As the practice of international criminal law based on the synthesis of common law and civil law standard (with a certain prevalence of common law), it is clear that there divergent interpretations in this area as well. It should be noted here that the negligent form of command responsibility is defined differently in the statutes of international criminal courts. The statutes of the ad hoc tribunals for Yugoslavia and Rwanda refer to the term „*had reason to know*",[47] while the Rome Statute deploys a somewhat different formulation of „*should have known*".[48] The practice of ad hoc tribunals sometimes excludes the possibility of negligence for command responsibility, which was the case in the *Bigilishema* judgment in which the ICTR warned that the „*references to „negligence" in the context of superior responsibility likely to lead to confusion of thought*".[49] This position was also expressly endorsed by the ICTY in the *Blaškić* judgment.[50] On the other hand, the practice of the ICC explicitly affirms that the *should have known* standard refers to negligence and that it is a different standard from *had reason to know* because the latter does not cover the duty of the commander to be familiar with the activities of their subordinates and that the breach of this duty automatically implies command responsibility.[51] This interpretation is largely accepted in literature as well.[52]

---

45 That is the case in Croatian jurisprudence, due to the fact that at the time of commiting these crimes, negligent form of command liability was not yet implemented in domestic law. See e.g. Supreme Court of the Republic of Croatia*, Case No. I Kž 397/2016*, 15 January 2019, p. 2. Serbian jurisprudence, however, *a limine* rejects the concept of superior responsibility, due to the same reason.

46 See e.g. Supreme Court of the Republic of Croatia*, Verdict No. I Kž 1008/2008-13,*18 November 2009.

47 ICTY Statute, Article 7 (3); ICTR Statute, Article 6 (3).

48 Rome Statute, Article 28 (a) (i).

49 *Supra* note 32, para. 35

50 *Prosecutor vs. Tihomir Blaškić*, Appeals Chamber Judgement (ICTY), Case No. IT – 95 – 14 – A, 29 Jul 2004, para. 63.

51 *Prosecutor vs. Jean-Pierre Bemba Gombo,* Pre-Trial Chamber II Decision (ICC), Case No. ICC-01/05-01/08, 15 Jun 2009, para. 429 - 434.

52 See Meloni, C., *Command Responsibility in International Criminal Law,* TMC Asser Press, Den Haag, 2010, pp. 183 – 184. For opposite standpoint see Martinez, *op. cit.,* note 29, pp. 660 – 664.

The elaboration above shows that the negligent standard of command responsibility is still controversial, unclear and difficult to prove. In the following sections, we will put this issue in the context of warfare with autonomous and semi-autonomous weapons and the command responsibility for violations of international warfare and humanitarian law committed through the use of such weapons. Currently, the most realistic situation is similar to the one that unfolded after the crash of the civilian airplane of Iran Air 655: the ATR gave the wrong information on the identification of the target, based on which the human hand gave the final command for the activation of the weapon which destroyed a civilian instead of a military target in violation of international criminal law (for example, committing a war crime). This issue has already captured the attention of certain authors who analyze it from the perspective of the violation of the principle of distinction between legal and illegal targets in warfare, as one of the key principles of international humanitarian law and warfare law. These authors warm that the Rome Statute requires intent of the perpetrator for command liability for war crimes, in the form of a conscious and willful targeting of civilian targets. requires. It is also questionable whether this includes *dolus eventualis* as well. According to these authors, it is not sufficient because in such cases, the cognitive activity of the human behind the machine is a result of an interaction with an autonomous system which is based on the reliance on the accuracy of the data provided by this system. However, this brings into question the interpretation according to which the human is not even aware of the risk of striking civilian targets (which is a constitutive characteristic of *dolus eventualis*), to which they allegedly consent. In this sense, there is also room to connect an error in fact, which is recognized by the Rome Statute as a legitimate ground for the exclusion of criminal liability. Therefore, these authors warn of a responsibility gap, which already exists in international criminal law related to warfare with autonomous weapons.[53] In addition, the jurisprudence of international criminal courts has applied a rigid interpretation of liability in the context of the destruction of civilian targets as a characteristic of war crimes. Thus, the ICC practice in this respect holds the position that the perpetrator must act with *dolus directus*.[54] The ICTY took a broader interpretation in such cases, allowing *dolus eventualis*[55] or even *recklessness*.[56]

---

53 Bo, M., *Autonomous Weapons and the Responsibility Gap in light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute*, Journal of International Criminal Justice, Vol. 19, No. 2, 2021. pp. 275 – 299.

54 *Prosecutor vs. Germain Katanga*, Trial Chamber II Judgement (ICC), Case No. ICC-01/04-01/07, 7 March 2014, para. 808.

55 *Prosecutor vs. Prlić et al,* Trial Chamber III Judgement (ICTY), Case No. IT – 04 – 74 – T, 29 May 2013, para. 192.

56 *Prosecutor vs. Stanislav Galić,* Trial Chamber III Judgement (ICTY), Case No. IT – 98 – 29 – T, 5 December 2003, para. 55.

Other authors, analyzing the issue of the applicability of the doctrine of command responsibility to crimes committed by autonomous weapons warn that the doctrine primarily relates to (superior and subordinate) persons, and not the relationship between humans and machines. If this doctrine would be applied to cases involving autonomous weapons, it would entail the application of legal rules such as *in dubio contra reum* and prohibited analogy, which is contrary to the fundamental criminal law postulates. Furthermore, command responsibility can exist only if there is a liability on the side of the subordinate perpetrators, which is also questionable in this case.[57] For these reasons, there are some proponents of a modified command responsibility according to the so-called „*dynamic diligence*" standard. According to this standard, the commander must ensure „*continual adjustments in the machine-human interface*", which will be conducted by adequately trained persons; must ensure that the assessments of the system were compatible with the standards of international humanitarian law; and ensure the „*flexibility in the parameters governing the machine's operation, with a presumption favoring interpretability of the AWS's outputs".* A failure to fulfill any of the listed duties would automatically lead to the criminal liability of the commander.[58] However, here one could ask the question of the approach if the commander undertakes the listed steps, but there are serious crimes and significant casualties regardless. In addition, it would be difficult to if not impossible to establish uniform technical standards for this type of maintenance and updating of the system, which would be the basis for the assessment of the commanders' compliance with the standard. Finally, it appears that the dynamic diligence criterium would open a lot of space for the invocation of the error of facts defense, thanks to the need for familiarity with advanced technologies, which requires advance knowledge, which most military commanders do not and must not possess. Therefore, this concept appears insufficiently clear at best and potentially impracticable. Other authors propose a significant reduction of the *mens rea* standard in the sense that a person will be considered liable if they are aware of the risk level of their conduct in principle, even if they are not conscious of (or willfully neglecting) the concrete source of this risk.[59] However, such an expansion of the *mens rea* standard would bring into question one of the fundamental principles of criminal law and it would indirectly introduce a strict liability of commanders. The issue will not be completely resolved either by the acceptance of

---

57 *Supra* note 15, pp. 140 – 146.

58 Margulies, P., *Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts*, in: Ohlin, J. D. (ed.), Research Handbook on Remote Warfare, Edward Elgar Press, Cheltenham – Northampton, 2019, pp. 405 – 442.

59 Jain, N., *Autonomous Weapons Systems: New Frameworks for individual Responsibility*, in: Bhuta, N. et al (eds.), Autonomous Weapons Systems: Law, Ethics, Policy, Cambridge University Press, Cambridge, 2016, p. 303.

the ideas of the proponents of the establishment of criminal liability of states, i.e. expanding criminal liability of legal entities in international criminal law.[60] Namely, this liability is not independent, but it also entails the liability of a (responsible) natural person, so the ultimate result will be the same.

Based on the foregoing, it can be concluded that the issue of the responsibility gap has been identified at the theoretical level, but there is no solution offered to date. On the other hand, practice has also not offered the interpretative criteria which would be useful in this context, especially with regards to the *should have known* standard which is more of a doctrinal than practical concept. It is clear that the fundamental principles of criminal law (the principle of liability, *in dubio pro reo* and the prohibition of analogy) are obstacles to a simple expansion and "adaptation" of the existing concept of command responsibility to situations of warfare with autonomous and semi-autonomous weapon systems. An additional issue is the causality of the (failure to) act of the commander, which is equally controversial in international and national practice of criminal law.[61] The situation in this respect will be even more difficult as the autonomy levels of these weapons increase, so it is conceivable in the near future that no legal system will be able to offer an adequate solution to the issue of command responsibility. Such a scenario is naturally unacceptable, especially taking into account the severity of the criminal offenses in question and their risk factor for the entire international community. Although weapons are increasingly built on autonomous artificial intelligence, it is a fact that victims remain human and there is a legal gap in this respect that can pose a great danger for the further development of modes of warfare. The emergence of wars without boundaries, with no liability and responsible persons are not permissible, which is why an adequate concept should be developed for the future. The next, final chapter of this paper will be dedicated to this issue.

4. CONCLUSION: AI COMMAND RESPONSIBILITY *DE LEGE FERENDA*?

The preceding elaborations show that none of the existing and proposed concepts provides an adequate and complete solution, which is why we endorse the position that the development of autonomous weapons should be halted.[62] At the

---

60 See more about that in *supra* note 15, pp. 146 – 150.

61 The problem of causality is, however, beyond the scope of this article. For more about that see e.g. Schabas, W. A., *The International Criminal Court, A Commentary on the Rome Statute,* Oxford University Press, Oxford – New York, 2010, pp. 461 – 462.

62 See e.g. Human Rights Watch, *Stopping Killer Robots, Country Positions on Baning Fully Autonomous Weapons and Retaining Human Control*, 2020, [https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and], Accessed 9 August 2022.

same time, we are aware of the fact that such a scenario is not likely because none of the major forces wants to lose the race to arms and the development of a powerful army, which would happen with the abandonment of autonomous weapons. Such a development is even more unrealistic taking into account the contemporary geopolitical situation in certain parts of the world, such as the war in Ukraine and the instability in certain parts of the world (Taiwan, Kosovo, etc). This is why there should be further efforts to develop an adequate concept of command liability. Here it is necessary to devise a model that will be accepted globally, and which would enable the creation of a minimum standard of rules going towards harmonization. This is very important if we take into consideration that the technological advancement of warfare is actually a global phenomenon.

The institute of command responsibility, even with the broadest possible interpretation of the *should have known* standard can suffice only in situations where a violation of an objectively determinable duty of the commander can be proven. This would include situations of the violation of the duty of regular maintenance and testing of the autonomous systema, a decision to use a system that is not sufficiently tested, or which is still in the experimental phase, entrusting the operation of the system to inadequately trained personnel, failure to organize an adequate training, different measures that hinder the safety of the operation of the system, etc. In the case of such violation, it would be possible to construe the legal standard of the violation of the duty of due care, which can be the basis for the negligent form of command responsibility (under the assumption that the judicial practice will be open such an interpretation. However, this institute will simply not be sufficient in situations where the commander invests all the necessary efforts, and especially if the weapon systems are fully autonomous (both in the phase of targeting and striking). In such cases the combined issues of the principles of liability, causality, and prohibited analogy will preclude criminal liability.

In order to overcome this issue, the only solution to the problem would be the introduction of a new (international) criminal offense of abstract endangerment, in which the zone of criminality would be moved one step forward so the commander would be liable only for a (bad) selection of autonomous weapon systems, which would cause an abstract danger for a protected object. The *Actus reus* of such a criminal offense would, at a minimum, entail the fulfillment of the following requirements: a) the perpetrator is a civil or military commander; b) in a *de iure* and *de facto* capacity to select the weapon; c) a decision to deploy the weapon in an area with a certain number of civilians and civil targets)which puts them in abstract danger) and d) the occurrence of certain consequences such as death, severe physical injury or destruction of civilian targets. The *mens rea* would consist of the awareness of the commander of the requirements a-c and their acceptance

of the abstract danger (a form of *dolus eventualis*), or their failure to raise awareness on the requirements, under the condition that the commander could have been and was aware of the requirements (a form of the *should have known* standard). It should be noted here that the *mens rea* could not include any subjective relationship towards the consequences under d) because this would imply command responsibility for war crimes. The described new criminal offense, which will be called *the endangerment of civilian targets by autonomous weapons,* would be less severe than the classic war crime, but at the same time, the range of the prescribed sentence would be broad be broad enough to adequately assess, in sentencing, the scope of the resulting consequences the danger of the act itself and the ensuing damage. This solution could, on the one hand, avoid the trap of the violation of the fundamental principles of criminal law, while at the same time, ensuring that the responsible persons bear the burden of responsibility. In addition, such a solution would have a solid basis in criminal policy because the choice of warfare with autonomous weapons entails the assumption of enhanced guarantee duties towards society and the international community at large.

Finally, we note that the aim of this paper is to foster future discussions on the development of an adequate model of command responsibility for crimes committed by autonomous weapon systems, in circumstances where it is unlikely that such a form of weapons will be stopped. This suggestion is susceptible to further modifications and expert dialogue from the *common law* and *civil law* legal tradition. However, the tendency should be towards a solution that would be acceptable from the perspective of international criminal law, which would also be in line with national legislation, in order to ensure that the perpetrators do not escape justice. In this sense, we hope that the dialogue on this topic will intensify in the forthcoming period.

REFERENCES

BOOKS AND ARTICLES

1. Amoroso, D., *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, Nomos, Napoli, 2020
2. Bassiouni, M. C., *Introduction to International Criminal Law*, *Second Revised Edition*, Brill-Nijhof, Leiden, 2014
3. Blomsma, J., *Fault elements in EU criminal law: the case for recklessness*, in: Klip, A. (ed.), Substantive Criminal Law of the European Union, Maklu, Antwerpen, 2011, pp. 135 – 159
4. Bo, M., *Autonomous Weapons and the Responsibility Gap in light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute*, Journal of International Criminal Justice, Vol. 19, No. 2, 2021. pp. 275 – 299

5. Bonafé, B. I., *Finding a Proper Role for Command Responsibility*, Journal of International Criminal Justice, Vol. 5, No. 3, 2007, pp. 599 – 618
6. Ching, A. B., *Evolution of the Command Responsibility Doctrine in Light of the Celebici Decision of the International Criminal Tribunal for the Former Yugoslavia,* North Carolina Journal of International Law, Vol. 25, No. 1, 1999, pp. 167 – 205
7. Gill, A. S., *The Role of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons,* UN Chronicle, Vol. 55, No. 4., 2019, pp. 15 – 17
8. Grut, C., *The challenge of autonomous lethal robotics to international humanitarian law*, Journal of Conflict and Security Law, Vol. 18, No. 1, 2013, pp. 5–23
9. Jain, N., *Autonomous Weapons Systems: New Frameworks for individual Responsibility*, in: Bhuta, N. et al (eds.), Autonomous Weapons Systems: Law, Ethics, Policy, Cambridge University Press, Cambridge, 2016, pp. 303-324
10. Jescheck, H.-H.; Weigend, T., *Lehrbuch des Strafrechts. Allgemeiner Teil,* Duncker & Humblot, Berlin, 1996
11. Margulies, P., *Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts*, in: Ohlin, J. D. (ed.), Research Handbook on Remote Warfare, Edward Elgar Press, Cheltenham – Northampton, 2019, pp. 405 – 442
12. Martinez, J. S., *Understanding Mens Rea in Command Responsibility*, Journal of International Criminal Justice, Vol. 5, No. 3, 2007, pp. 638-664
13. Matthias, A., *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata,* Ethics and Information Technology, Vol. 6, No. 3, 2004, pp. 175 - 183
14. Mauri, D., *Autonomous Weapons Systems and the Protection of Human Persons – An International Law Analysis*, Edward Elgar Publishing, Cheltenham – Northampton, 2022
15. Meloni, C., *Command Responsibility in International Criminal Law,* TMC Asser Press, Den Haag, 2010
16. Postma, J., *Drones over Nagorno-Karabakh,* Atlantisch Perspectief , Vol. 45, No. 2, 2021, pp. 15–20
17. Satzger, H., *International and European Criminal Law,* C. H. Beck – Hart – Nomos, München – Oxford, 2012
18. Schabas, W. A., *The International Criminal Court, A Commentary on the Rome Statute,* Oxford University Press, Oxford – New York, 2010
19. Scharre, P., *Centaur Warfighting: The False Choice of Humans vs. Automation,* Temple International and Comparative Law Journal, Vol. 30, No. 1, 2016, pp. 151-165

INTERNATIONAL CRIMINAL COURT

1. *Prosecutor vs. Germain Katanga*, Trial Chamber II Judgement (ICC), Case No. ICC-01/04-01/07, 7 March 2014
2. *Prosecutor vs. Jean-Pierre Bemba Gombo,* Pre-Trial Chamber II Decision (ICC), Case No. ICC-01/05-01/08, 15 June 2009

INTERNATIONAL CRIMINAL TRIBUNAL FOR RWANDA

1. *Prosecutor vs. Bagilishema,* Appeals Chamber Judgement (ICTR), Case No. ICTR – 95 – 1A-A, 3 July 2002

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA

1. *Prosecutor vs. Prlić et al,* Trial Chamber III Judgement (ICTY), Case No. IT – 04 – 74 – T, 29 May 2013
2. *Prosecutor vs. Stanislav Galić,* Trial Chamber III Judgement (ICTY), Case No. IT – 98 – 29– T, 5 December 2003
3. *Prosecutor vs. Tihomir Blaškić*, Appeals Chamber Judgement (ICTY), Case No. IT – 95 – 14 – A, 29 July 2004

INTERNATIONAL DOCUMENTS

1. UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998
2. UN Security Council, Statute of the International Criminal Tribunal for Rwanda (as last amended on 13 October 2006), 8 November 1994
3. UN Security Council, Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 17 May 2002), 25 May 1993

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Croatian Criminal Code, Official Gazette No. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022
2. Völkerstrafgesetzbuch, BGBl. I S. 2254, BGBl. I S. 3150
3. Supreme Court of the Republic of Croatia, Verdict No. I Kž 1008/2008-13, 18 November 2009
4. Supreme Court of the Republic of Croatia, Case No. Kž-rz 22/2018
5. Supreme Court of the Republic of Croatia, Case No. I Kž 397/2016, 15 January 2019

REPORTS

1. Boulanin, V.; Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems*, SIPRI, Solna, 2017
2. American Law Institute, Model Penal Code, 1962

WEBSITE REFERENCES

1. Simple Flying, *34 Years Ago Today: The Shootdown Of Iran Air Flight 655*, 2022, [https://simpleflying.com/iran-air-flight-655-1988-shootdown-anniversary/], Accessed 27 July 2022

2. European Parliament, *Eurpean Parliament Resolution of 16 February 2011 on the 2010 progress report on Croatia*, [https://www.europarl.europa.eu/doceo/document/TA-7-2011-0059_EN.pdf], Accessed 1 August 2022
3. Human Rights Watch, *Stopping Killer Robots, Country Positions on Baning Fully Autonomous Weapons and Retaining Human Control*, 2020, [https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and], Accessed 9 August 2022
4. HAROP, *Loitering Munition System*, [https://www.iai.co.il/p/harop], Accessed 28 July 2022
5. The Messenger, *The Ukraine War in data: Winning the drone war*, [https://www.grid.news/story/global/2023/01/05/the-ukraine-war-in-data-winning-the-drone-war/], Accessed 13 February 2023
6. UK Ministry of Defence, *Joint Doctrine Publication 0-30.2., Unmaned Aircraft Systems*, 2017,[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf], Accessed 28 July 2022
7. United Nations Institute for Disarmament Research (UNIDIR), *Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies*, Geneva, 2016, [https://unidir.org/publication/safety-unintentional-risk-and-accidents-weaponization-increasingly-autonomous], Accessed 28 July 2022
8. US Department of Defense, *Directive No. 3000.09*, 2017, [https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf], Accessed 28 July 2022

UDK 336.74-021.131:339.72
Review article

WHEN IS A CRYPTOCURRENCY TRANSFER INTERNATIONAL IN DISTRIBUTED LEDGER TECHNOLOGY-BASED SYSTEMS?*

Burcu Yüksel Ripley, PhD, Senior Lecturer
University of Aberdeen, School of Law
High Street, Aberdeen, AB24 3UB, United Kingdom
b.yuksel@abdn.ac.uk

ABSTRACT

Cryptocurrencies, introduced in 2009 with the first cryptocurrency, Bitcoin, have grown significantly in recent years and attracted attention globally. One of the main characteristics of cryptocurrencies and their key innovation is that they are underpinned by distributed ledger technology (DLT) or blockchain as a type of DLT. This technology enables cryptocurrencies to be transferred, stored or traded electronically within DLT-based systems in a peer-to-peer manner among (pseudonymous) system participants across the world without the involvement of the usual central trusted authorities or intermediaries such as banks. This raises the question of if, and how, one should ascertain internationality for cryptocurrency transfers taking place within truly global systems underpinned by DLT for private international law purposes.

This article aims to raise awareness of and address the question of internationality in the context of cryptocurrency transfers in DLT-based systems. It considers internationality in private international law, potential factors that might be relevant in ascertaining internationality for cryptocurrency transfers through a comparison to that for electronic funds transfers (EFTs), and the approaches of the International Institute for the Unification of Private Law (UNIDROIT) and the Hague Conference for Private International Law (HCCH) on internationality in their current projects concerning digital assets and digital economy respectively.

Keywords: *Blockchain, cryptocurrency, distributed ledger technology, foreign element, internationality, private international law*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

Cryptocurrencies, introduced in 2009 with the first cryptocurrency Bitcoin,[1] have grown significantly in recent years and attracted attention globally. They now represent a sub-category of cryptoassets, which are mainly used as a means of exchange but are not state backed,[2] under the broader umbrella of digital assets that accommodate different types of assets emerging with the use of technology.

One of the main characteristics of cryptocurrencies and arguably their key innovation is that they are underpinned by distributed ledger technology (DLT) or blockchain as a type of DLT.[3] This technology enables cryptocurrencies to be transferred, stored or traded electronically within DLT-based systems in a peer-to-peer manner among system participants across the world without the involvement of the usual central trusted authorities or intermediaries such as banks.[4] Transactions are directly made between the respective participants after being verified and validated by other participants in the system (known as miners in Bitcoin) according to consensus rules or protocols.[5] This technology also enables secure digital records in relation to those transactions to be held at a ledger distributed across the system, allowing system participants to have an identical copy of the ledger and precluding the ledger being modified by a participant secretly.[6] DLT-based systems represents a significant shift from intermediation to disintermediation and from centralised ledgers to not only decentralised but also distributed ledgers.[7] This can potentially transform many areas and sectors which have traditionally operated

---

1 See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

2 See e.g. UK Cryptoassets Taskforce, *Final report*, 2018, pp. 11-15, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf], Accessed 1 February 2023.

3 Ali, R.; Barrdear, J.; Clews, R.; Southgate, J., *Innovations in Payment Technologies and the Emerge of Digital Currencies,* Bank of England Quarterly Bulletin, Vol. 54, 2014, pp. 262-275, p.262.

4 See generally Geva, B., *Banking in the Digital Age- Who is Afraid of Payment Disintermediation*, EBI Working Paper Series, No. 23, 2018.

5 UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts*, 2019, par. 30, [https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf], Accessed 1 February 2023.

6 See de Caria, R., *A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities*, *Modernizing International Trade Law to Support Innovation and Sustainable Development* UNCITRAL, 2017, p. 106, [https://aperto.unito.it/retrieve/handle/2318/1632525/464608/R.%20de%20Caria%2c%20A%20Digital%20Revolution%20%282017%29.pdf], Accessed 1 February 2023.

7 For the advantages that DLT-based systems offer, see e.g., Yüksel, B.; Heindler, F., *Use of Blockchain Technology in Cross-Border Legal Cooperation under the Conventions of the Hague Conference on Private International Law (HCCH)*, Aberdeen Law School Blog, 2019, [https://www.abdn.ac.uk/law/blog/use-of-blockchain-technology-in-crossborder-legal-cooperation-under-the-conventions-of-the-hague-conference-on-private-international-law-hcch/], Accessed 1 February 2023.

based on intermediation and with centralised ledgers, and can have a wide range of applications including, but not limited to, cryptocurrencies.[8]

DLT raises several private international law issues, particularly in the determination of international jurisdiction and applicable law. In relation to cryptocurrencies, as identified by the Hague Conference on Private International Law (HCCH), these issues include the law applicable to cryptoassets,[9] the law applicable to transfers of cryptoassets on a blockchain and outside a blockchain, the determination of international jurisdiction, and party autonomy in respect of jurisdiction and applicable law.[10] The traditional private international law questions with respect to international jurisdiction and applicable law get more complicated in the context of cryptocurrencies given that cryptocurrency systems underpinned by DLT or blockchain 'do not recognise traditional national borders and have global reach'[11] and can have pseudonymous system participants whose true identities are not known and not disclosed to each other. This raises the question of if, and how, one should ascertain internationality for cryptocurrency transfers in DLT-based systems for private international law purposes, which is a question that has not attracted much attention yet.

This article aims to raise awareness of and address the question of internationality in the context of cryptocurrency transfers in DLT-based systems by considering internationality in private international law, potential factors that might be relevant in ascertaining internationality for cryptocurrency transfers through a comparison to that for electronic funds transfers (EFTs), and the approaches of the International Institute for the Unification of Private Law (UNIDROIT) and the HCCH on internationality in their current projects concerning digital assets and digital economy respectively including cryptocurrencies.

2. INTERNATIONALITY IN PRIVATE INTERNATIONAL LAW

It might be best to start the analysis with the question of why internationality matters, before addressing what internationality means and how it is defined. In-

---

8 See e.g. HCCH, *Proposal for the Allocation of Resources to Follow Private International Law Implications relating to Developments in the Field of Distributed Ledger Technology*, in particular in relation to 'Financial Technology', Preliminary Document 28 February 2020, par. 8., [https://assets.hcch.net/docs/f787749d-9512-4a9e-ad4a-cbc585bddd2e.pdf], Accessed 1 February 2023.

9 On this issue, see Yüksel Ripley, B.; Heindler, F., *The Law Applicable to Cryptoassets: What Policy Choices are ahead of us* in Bonomi, A.; Lehmann, M; Lalani S. (eds.), *Distributed Ledger Technologies and Private International Law*, Brill, forthcoming.

10 HCCH, *op. cit.,* note 8, pars. 10-15.

11 *Ibid.*, par. 9.

ternationality matters because when a transaction, relationship or situation is international or, in private international law jargon, involves a foreign element, this means that that transaction, relationship or situation is no longer contained in the domestic arena. Different laws and jurisdictions then potentially become relevant to that transaction, relationship or situation. It is the very essence of the existence of private international law, as a discipline, to resolve the conflict of jurisdictions and the conflict of laws in such cases by determining a court of the competent jurisdiction to hear disputes arising from that transaction, relationship or situation and the law applicable to them to resolve the substance of the disputes.

In private international law, a foreign element is generally understood as an element that connects a transaction, relationship or situation to more than one legal system.[12] It is this foreign element that a transaction, relationship or situation involves which triggers a private international law analysis. This foreign element traditionally derives from the persons (such as the party's nationality) or the places/locations (such as the place of performance) concerned.[13]

A distinction is made by some, particularly in the field of contracts, between situations with a foreign element and situations of an international character.[14] However, there is no agreement in private international law on the criteria that would give a transaction, relationship or situation an international character. Arguments on this matter, mainly raised in relation to contracts, seem to differ from one legal system to another and by time.[15] In general, the international character of a transaction, relationship or situation can be determined based on an objective, economic or subjective test,[16] and different factors can have varying importance and weight in this determination depending on the nature of a given transaction,

---

12 See e.g. See Lord Collins of Mapesbury *et al.*, *Dicey, Morris & Collins on the Conflict of Laws*, 15th ed, Sweet and Maxwell, 2014, pars. 1-001- 1-002.

13 See e.g. Nomer, E., *Devletler Hususi Hukuku*, 21st ed., İstanbul, Beta, 2015, p. 5; Tekinalp, G.; Uyanık, A., *Çavuşoğlu*, *Milletlerarası Özel Hukuk Bağlama Kuralları*, 12th ed., İstanbul, Vedat, 2016, p.18.

14 von Hoffmann, B., *General Report on Contractual Obligations* in Lando, O.; von Hoffmann, B.; Siehr, K. (eds.), *European Private International Law of Obligations*, Tübingen, J.C.B. Mohr (Paul Siebeck), 1975, pp. 1-41, pp. 15-17; Collins, L., *Contractual Obligations- The ECC Preliminary Draft Convention on Private International Law*, International and Comparative Law Quarterly, Vol. 25, No.1, 1976, pp. 35-57, p. 41.

15 See Lando, O., *International Situations and Situations Involving a Choice between the laws of Different Legal Systems*, in Lipstein, K. (ed), *Harmonization of private international law by the E.E.C*, London, Institute of Advanced Legal Studies, 1978, pp. 15-24, p. 19; Lando, O., *The Conflict of Laws of Contracts: General Principles*, Recueil des Cours, Vol. 189, 1984, pp. 225-447, pp. 286-287.

16 For an analysis on these tests, see Nygh, P., *Autonomy in International Contracts*, OUP, 1999, pp. 48-55.

relationship or situation.[17] For example, the nationality of the parties can possibly have greater importance in the law of persons compared to the law of contracts.

Internationality should not be seen merely as a theoretical question. It plays an important role in defining and determining the scope of application of legal instruments through different techniques and approaches.[18] For example, Article 1(1) of the HCCH 2005 Choice of Court Agreements Convention[19] limits its scope of application to international cases and provides a negative definition of internationality by excluding purely domestic cases.[20] According to Article 1(2), for the purposes of jurisdictional rules of the Convention, 'a case is international unless the parties are resident in the same Contracting State and the relationship of the parties and all other elements relevant to the dispute, regardless of the location of the chosen court, are connected only with that State'. The Explanatory Report of the Convention illustrates the internationality via an example where parties choose a court in Japan for a contract which is made in Portugal between parties both residing in Portugal and to be performed in Portugal.[21] Such a case is not considered international under the Convention since all elements are connected to Portugal except for the location of the chosen court.[22] Primarily inspired by Article 1(2) of the HCCH 2005 Choice of Court Agreements Convention, the HCCH 2015 Principles on Choice of Law in International Commercial Contracts[23] also provides a negative definition of internationality for contracts in Article 1(2) by excluding contracts where 'each party has its establishment in the same State and the relationship of the parties and all other relevant elements, regardless of the chosen law, are connected only with that State'.[24] According to the

---

17 Regarding contracts, see Delaume, G. R., *What is an International Contract? An American and a Gallic Dilemma*, International and Comparative Law Quarterly, Vol. 28, No.2, 1979, pp. 258-279, p. 279.

18 See Kronke, H., *Connecting Factors and Internationality in Conflict of Laws and Transnational Commercial Law*, in *Boele-Woelki*, K.; *Einhorn*, T.; *Girsberger, D.; Symeonides, S. (eds.), Convergence and Divergence in Private International Law– Liber Amicorum Kurt Siehr*, The Hague– Zürich, Eleven International Publishing – Schulthess, 2010, pp. 57-70, pp. 67-69.

19 Convention on Choice of Court Agreements, 30 June 2005.

20 Hartley, T.; Dogauchi M., *Explanatory Report of the Convention of 30 June 2005 on Choice of Court Agreements*, HCCH, par. 11, [https://www.hcch.net/en/publications-and-studies/details4/?pid=3959&dtid=3], Accessed 1 February 2023. (Hartley/Dogauchi Report). See also Weller, M., *Choice of court agreements under Brussels Ia and under the Hague Convention: Coherences and clashes*, Journal of Private International Law, Vol. 13, No. 1, 2017, pp. 91-129, pp. 93-97.

21 *Ibid.*, par. 42. The illustration assumes that the Convention is in force in the States mentioned therein.

22 *Ibid.*

23 HCCH, *Principles on Choice of Law in International Commercial Contracts*, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=135], Accessed 1 February 2023.

24 See par. 1.14 of the Commentary of the HCCH 2015 Principles on Choice of Law in International Commercial Contracts, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=135], Accessed 1 February 2023.

Commentary, the exclusion of only purely domestic situations from the definition of internationality reflects the aim of conferring 'the broadest possible scope of interpretation to the term 'international''.[25]

The HCCH 1986 Convention on the Law Applicable to Contracts for the International Sale of Goods,[26] on the other hand, provides a positive definition of internationality[27] and identifies its scope of application in Article 1 as contracts 'a) between parties having their places of business in different States; b) in all other cases involving a choice between the laws of different States, unless such a choice arises solely from a stipulation by the parties as to the applicable law, even if accompanied by a choice of court or arbitration'.[28] The HCCH 2006 Securities Convention[29] adopts a broad descriptive approach to internationality[30] in Article 3 by referring to 'all cases involving a choice between the laws of different States'.[31] This is to ensure the Convention's applicability 'unless there is absolutely no element in the facts of a case (e.g., 'location' of a person involved in or affected by a transaction or of an activity of such a person, 'location' of a security or its issuer, presence of a governing law clause or any other 'governing law' factor or element) that might require a decision as to which of two or more legal systems is applicable'.[32] It is interesting to note that the Explanatory Report of the Convention seems to suggest a distinction between a foreign element and internationality in respect of the Convention's applicability.[33] Based on the Explanatory Report, although the title of Article 3 is internationality, the text of it does not use the term intentionally so that situations which appear at first glance to be wholly internal are still covered by the Convention due to the foreign element they involve.[34] The Rome

---

25 *Ibid*.

26 Convention on the Law Applicable to Contracts for the International Sale of Goods, 22 December 1986.

27 For this interpretation, see par. 1.15 of the Commentary of the HCCH 2015 Principles on Choice of Law in International Commercial Contracts, *op. cit.,* note 24.

28 For further information on internationality in the scope of this Convention, see von Mehren, A. T., *Explanatory Report of the Convention on the Law Applicable to Contracts for the International Sale of Goods*, HCCH, 1987, pars 21-25.

29 Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, 5 July 2006.

30 Goode, R.; Kanda, H.; Kreuzer K. with the assistance of Bernasconi C., *Hague Securities Convention Explanatory Report*, HCCH, 2017, par. 3-3.

31 The term 'cases' is understood as 'situations' in this context, see *ibid.*, par. 3-12.

32 *Ibid.*, par. 3-12.

33 *Ibid.*, par. 3-4.

34 *Ibid.*

I Regulation on the law applicable to contractual obligations,[35] applied in the European Union (EU) and retained by the United Kingdom (UK)[36] post-Brexit, also provides a broad approach to internationality by defining the Regulation's scope of applicability to 'situations involving a conflict of laws' in Article 1(1)'.

Internationality is considered as a requirement which is 'consistent with the traditional understanding that private international law applies only to international cases'.[37] Therefore, although its definition can vary considerably among legal instruments, there is typically a definition or test for internationality to be satisfied under the legal instruments.

3. INTERNATIONALITY OF CRYPTOCURRENCY TRANSFERS IN DISTRIBUTED LEDGER TECHNOLOGY BASED-SYSTEMS

Based on the analysis in chapter II of this article, for a cryptocurrency transfer to be subject to a private international law analysis, there needs to be an element that gives the transfer an international character. The question therefore arises as to if, and how, such an element will be ascertained in cryptocurrency transfers taking place within truly global systems underpinned by DLT to trigger a private international law analysis.

3.1. Ascertainment of Internationality

A distinction can be made between a transfer involving a foreign element and a transfer being international for private international law purposes.[38] Cryptocurrency systems underpinned by DLT would ordinarily and unavoidably involve a foreign element since these systems have participants located in different jurisdictions and the ledger, distributed across the system participants, exist potentially in many places.[39]

---

35 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6 (Rome I Regulation).

36 The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/834) as amended by the Jurisdiction, Judgments and Applicable Law (Amendment) (EU Exit) Regulations (SI 2020/1574).

37 Par. 1.13 of the Commentary of the HCCH 2015 Principles on Choice of Law in International Commercial Contracts, *op. cit.,* note 24.

38 For an argument in favour of the same distinction regarding EFTs, see Yüksel, B., *Uluslararası Elektronik Fon Transferine Uygulanacak Hukuk*, XII Levha, 2018, p. 39-40.

39 For the argument that if a smart contract is operated on a blockchain that involves nodes across various jurisdictions, this should be considered as a sufficient connection to a foreign country, see Rühl, G., *Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?* in Cappiello, B.; Carulo, G. (eds.), *Blockchain, Law and Governance*, eBook, Springer, 2021, pp. 159-180, pp. 163-164.

One might therefore argue that all cryptocurrency transfers within DLT-based systems are international.[40]

However, there may be examples which indicate otherwise. For example, Bitcoin is accepted as a form of payment, to different extents, in various countries in shops, bars and cafes.[41] Although Bitcoin transfers take places within the Bitcoin system underpinned by blockchain and are executed with the involvement of miners who informally work in a peer-to-peer manner as transaction verifiers and bookkeepers around the world with no central coordination,[42] a Bitcoin transfer to make a payment between the two parties located in the same jurisdiction is in essence a domestic transfer, not an international one. Cryptocurrencies are also used and give rise to legal questions in other wide-ranging matters, including family[43] and succession matters, in purely domestic situations as well. On this basis, the mere fact that a cryptocurrency transfer is executed within a DLT system may not be sufficient on its own to give a cryptocurrency transaction an international character.

The question of internationality has been raised in respect of EFTs too.[44] An EFT is the movement of funds between different bank accounts by electronic means.[45] It is in essence the transfer of value without the need of a physical transfer of money[46] and, whilst this resembles a cryptocurrency transfer, the way that EFTs and cryptocurrencies are executed is significantly different.[47] In a typical EFT, there

---

40 See e.g. Guillaume who argues that, given the role of the nodes in the network, the use of the blockchain is sufficient to give blockchain transactions an international scope and that it is statistically unlikely that all the nodes in the network or involved in a given transaction will be located in the same state, Guillaume, F., *Aspects of private international law related to blockchain transactions*, in Kraus, D.; Obrist, T.; Hari, O. (eds.), *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, Cheltenham/Northampton, Edward Elgar, 2019, pp. 49-82; p. 59.

41 For the UK, see e.g. UK Cryptoassets Taskforce Final report, *op. cit.*, note 2, par. 2.18.

42 See generally, Ali; Barrdear; Clews; Southgate, *op. cit.,* note 3, p. 266 and 268.

43 See e.g. Hodson, D., *Cryptocurrency and the Family Courts – Some International Experiences*, Financial Remedies Journal, No. 1, 2023.

44 See generally Yüksel, *op. cit.,* note 38*,* 41-47.

45 For different definitions of EFT having this similar core, see e.g., Geva, B., *The Law of Electronic Funds Transfers*, Matthew Bender, 1994, par. 1-26; Karageorgiou, S., *Electronic Funds Transfers: Technical & Legal Overview*, Thesis, University of London Queen Mary and Westfield College, 1990, page 33; Proctor, C., *The Law and Practice of International Banking*, 2nd ed, OUP, 2015, par. 19.05; United Nations Commission on International Trade Law, *UNCITRAL Legal Guide on Electronic Funds Transfers*, 1987, [www.uncitral.org/pdf/english/texts/payments/transfers/LG_E-fundstransfer-e.pdf] ('UNCITRAL Legal Guide'), Accessed 1 February 2023.

46 Cox, R.; Taylor, J., *Funds Transfer* in Brindle, M.; Cox, R. (eds.), *Law of Bank Payments*, Sweet & Maxwell, 2017, par. 3-002; Ellinger, E. P; Lomnicka, E.; Hare, C. V. M, *Modern Banking Law*, 5th ed, OUP, 2011, p. 559.

47 Yüksel Ripley, B., *Cryptocurrency Transfers in Distributed Ledger Technology-Based Systems and Their Characterisation in Conflict of Laws* in Borg-Barthet, J.; Trimmings, K.; Yüksel Ripley, B.; Živković,

are separate bank accounts and the amount is transferred from one to another by adjusting the balances of the relevant bank accounts via debiting the amount from one account and crediting it to another.[48] This process involves clearing and settlement either on a bilateral basis between the two respective banks that are correspondents holding an account with the other[49] or on a multilateral basis on the books of a common correspondent bank or of a central bank in a funds transfer system.[50] Given the reliance on centralisation and intermediation, the suggested definition or test of internationality for EFTs is usually based on the location of banks. For example, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on International Credit Transfers,[51] which only applies to international transfers, adopts a test of internationality in Article 1(1) based on the location of banks by defining its sphere of application as 'credit transfers where any sending bank and its receiving bank are in different States'.[52] If these banks are in different states, the transfer is therefore international. In legal literature, the definition of international funds transfer, which has been given by Professor Geva and adopted by many others, indicates a similar approach to internationality by accepting 'any transfer of funds involving either banks located in more than one country or at least one bank located in a country other than that of the currency of the transfer' as an international funds transfer.[53]

However, such a definition or test for internationality for EFTs based on the location of banks does not seem directly applicable to cryptocurrency transfers since there is no bank or similar trusted third party that executes the transfers and records them to the ledger in DLT-based systems. This is done on a peer-to-peer basis by miners or trusted nodes in those systems which rely on distributed ledgers and disintermediation. Ascertaining internationality based on the location of miners or trusted nodes

P. (eds.), *From Theory to Practice in Private International Law: Gedächtnisschrift for Professor Jonathan Fitchen*, Oxford, Hart Publishing, forthcoming.

48 Cox; Taylor, *op. cit.,* note 46, par. 3-002; Ellinger; Lomnicka; Hare, *op. cit.,* note 46, 559.

49 Geva, *op. cit*., note 45, par. 1-28; Ellinger; Lomnicka; Hare, *op. cit.* note 46, 464; Malek, A.; Odgers, J.*, Paget's Law of Banking*, 14th ed, Lexis Nexis, 2014, par. 22.32.

50 Geva, *op. cit.,* note 45, 1-28; Ellinger; Lomnicka; Hare, *op. cit.,* note 45, 564; Malek; Odgers, *op. cit.,* note 49, par. 22.32.

51 UNCITRAL, *The UNCITRAL Model Law on International Credit Transfers*, 1992, [https://uncitral.un.org/en/texts/payments/modellaw/credit_transfers], Accessed 1 February 2023.

52 See UNCITRAL, *Explanatory Note on the UNCITRAL Model Law on International Credit Transfers*, 1992, par. 12, [https://uncitral.un.org/en/texts/payments/modellaw/credit_transfers], Accessed 1 February 2023. See also Yüksel, B., *Facilitating International Trade between Turkey and China by International Payments via Electronic Funds Transfer: Problems and Possible Solutions under the UNCITRAL Model Law on International Credit Transfers* in Yenidünya, C.; Erkan, M.; Asat, R. (eds.), *Reopening the Silk Road in the Legal Dialogue Between Turkey and China*, Ankara, Adalet, 2013, pp. 365-393, p. 381.

53 Geva, *op. cit.,* note 45, par. 4-5.

would not be feasible either since their location is usually unknown in pseudonymous systems and is also coincidental.[54] Therefore, such ascertainment might lead to unexpected results for the parties of the transaction. Location of the transferor and the transferee, on the other hand, can be considered as a criterion for internationality for cryptocurrency transfers if those locations are known or identifiable. Accordingly, a transfer of cryptocurrency in DLT-based systems can be regarded international if the parties of the transfer are located in different countries. Alternatively, the internationality of a cryptocurrency transfer can be subject to the internationality of the underlying relationship between the parties of the transfer.

3.2. Approaches of the UNIDROIT and the HCCH to Internationality

There are currently two important legal initiatives at the international level, by the UNIDROIT and the HCCH, which aim to address aspects of digital assets and digital economy including cryptocurrencies. However, it is not clear whether the UNIDROIT and the HCCH take a particular approach to internationality in this context and, if they do, what that approach is.

3.2.1. UNIDROIT Project on Digital Assets and Private Law

The UNIDROIT has conducted a project on Digital Assets and Private Law,[55] which resulted in the adoption of the UNIDROIT Principles on Digital Assets and Private Law in May 2023 following a public consultation[56]. At the time of writing of this article, the UNIDROIT Secretariat, mandated by the Governing Council, is working towards the final publication of the instrument and the most up-to-date draft of the Principles is available in the Annexe to the Governing Council document on the Principles on Digital Assets and Private Law.[57] The draft UNIDROIT Principles consist of 19 principles, each accompanied by

---

[54] *cf.* Garriga Suau who argues that a criterion based on the location of the nodes can be considered for internationality in relation to permissionless blockchains unless the terms and conditions of the blockchain network specify otherwise regarding the internationality of its network, see Garriga Suau, G., *Blockchain-based smart contracts and conflict rules for business-to-business operations*, *Revista Electrónica de Estudios Internacionales, Vol. 41, 2021, pp. 1-27, pp. 22-23. cf.* also Guillaume, *op. cit.,* note 40.

[55] See UNIDROIT, *Digital Assets and Private Law: Study LXXXII Digital Assets and Private Law Project,* [https://www.unidroit.org/work-in-progress/digital-assets-and-private-law], Accessed 1 February 2023.

[56] See UNIDROIT, *Digital Assets and Private Law- Public Consultation,* [https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/digital-assets-and-private-law-public-consultation], Accessed 1 February 2023.

[57] See UNIDROIT, *Item No. 4 on the agenda: Adoption of Draft UNIDROIT Instruments (c) Principles on Digital Assets and Private Law*, 2023, pp. 10- 77, [https://www.unidroit.org/wp-content/uploads/2023/04/C.D.-102-6-Principles-on-Digital-Assets-and-Private-Law.pdf], Accessed 31 July 2023.

commentary, and one of these principles, ie Principle 5, deals with the applicable law under Section II entitled private international law.

Section I of the draft UNIDROIT Principles considers scope and definitions. According to illustration 1 in commentary 2.8, 'virtual (crypto) currency on a public blockchain (e.g. bitcoin) is a digital asset'. Principle 1 sets out the scope of application as 'the private law relating to digital assets'. When this is read along the Commentary, it seems that this material scope of application is limited to only certain aspects of private law, in particular property law and insolvency law.[58] A number of proprietary issues are excluded from the material scope in Principle 3(3). It is interesting to note that the material scope of Principle 5 on the applicable law, on the other hand, is not limited to the issues covered by the Principles.[59] This is a rather unusual technique as the scope of the provision has a wider scope of application than the instrument it is included in, which raises further questions concerning the relationship between the application of Principle 5 on the applicable law and this UNIDROIT instrument as a whole.[60]

Although the material scope of application is defined in Section I of the draft UNIDROIT Principles, the territorial scope of application is not explicitly defined therein or elsewhere in the Principles. Based on commentary 0.4, it can be inferred that the draft UNIDROIT Principles have been designed to apply in both domestic and international (or cross-border) situations[61] given references therein to transactions involving digital assets that occur in a State and transactions involving persons in different States respectively. It is however not clear what counts as an international (or cross-border) situation for the purposes of these Principles although this requirement or test of internationality becomes particularly important for the application of Principle 5 on the applicable law.[62] The question therefore arises as to whether all situations relating to proprietary issues in respect of a digital asset are deemed international (or cross-border) under the UNIDROIT Principles and require a conflict of law analysis.[63]

---

58 See Yüksel Ripley, B.; MacPherson, A.; Poesen, M.; Albargan, A.; Xuan Tung, L., *The response of the Centre for Commercial Law at the University of Aberdeen to the UNIDROIT Digital Assets and Private Law Consultation*, February 2023, p. 2, [https://www.abdn.ac.uk/law/research/centre-for-commercial-law/public-policy-stakeholder-engagement-1109.php], Accessed 21 February 2023.

59 See commentary 5.2, *op. cit.,* note 57.

60 See Yüksel Ripley, *et al.*, *op. cit.,* note 58, p. 4.

61 See *ibid.*, p. 2.

62 *Ibid.*, p. 2 and 5.

63 *Ibid.*, p. 5.

Internationality is also important from the point of choice of law rules provided in Principle 5 which grants parties the power to choose the applicable law.[64] There is no consensus in private international law on the question of whether parties should be allowed to choose the applicable law for domestic situations.[65] Internationality is seen as the most common of the parameters and limitations that the principle of party autonomy is subject to in modern private international law codifications and conventions.[66] This typically may result in parties not being permitted a choice of law for domestic transactions at all, or such choices are accommodated not strictly as a choice of law but, for example, as an incorporation by reference of the provisions of that foreign law into the parties' contract, with or without an express subordination to the mandatory rules of the country with which the situation is wholly connected.[67] At the stage of the public consultation, it was assessed in relation to the draft UNIDROIT Principles that allowing an unlimited choice of law for domestic transactions would be hard to justify under these considerations and it was suggested that providing 'a presumption of internationality for transactions in digital assets, which could be rebutted in exceptional cases, e.g. a permissioned network limited to participants established in the same country' could address this issue.[68]

---

64 See EAPIL Working Group on the Law Applicable to Digital Assets, *The position paper of the European Association of Private International Law (EAPIL) in response to the public consultation on the UNIDROIT Draft Principles and Commentary on Digital Assets and Private Law issues*, 2023, par. 15, [https://eapil.org/wp-content/uploads/2023/03/EAPIL-WG-Digital-Assets-Position-paper-March-2022-Final.pdf], Accessed 20 March 2023.

65 See generally Mills, A., *Party Autonomy in Private International Law*, CUP, 2018, pp. 470-476. See also Ostendorf, P., *The choice of foreign law in (predominantly) domestic contracts and the controversial quest for a genuine international element: potential for future judicial conflicts between the UK and the EU?*, Journal of Private International Law, Vol. 17, No. 3, 2021, pp. 421-438.

66 On this point regarding party autonomy in contract conflicts, see Symeonides, S. C., *Codifying Choice of Law Around the World: An International Comparative Analysis,* OUP, 2014, pp. 116-117. See also Albornoz, M.; Gonzalez Martin, N., *Towards the uniform application of party autonomy for choice of law in international commercial contracts*, Journal of Private International Law, Vol. 12, No. 3, 2016, pp. 437-465, pp. 440-443.

67 See *ibid*. For a comparative analysis between Turkish and EU private international law on this matter, see also Yüksel, B., *Choice of Law in Civil and Commercial Matters under Turkish Private International Law in Comparison with their Equivalents under the Rome I and Rome II Regulations,* in Beaumont, P.; Yüksel, B. (eds.), *Turkish and EU Private International Law: A Comparison*, Istanbul, XII Levha, 2014, pp. 153-223, pp. 165-166.

68 EAPIL, *op. cit.,* note 63, par. 15. See also the argument for an assumption that 'all blockchain transactions must be considered international by nature' unless 'all nodes, all the users, as well as the operator of the blockchain are located in the same State' by Guillaume, *op. cit.,* note 40.

3.2.2. HCCH Work on Private International Law Implications of the Digital Economy

The HCCH has been closely following the developments with respect to private international law implications of the digital economy including DLT and its certain applications since 2020.[69] The HCCH has also been closely cooperating and coordinating, including through participation as an observer, with the UNCITRAL and UNIDROIT in relation to their work in this area including the UNIDROIT's project on Digital Assets and Private Law.[70] As an intergovernmental organisation working with the mandate of the progressive unification of the rules of private international law,[71] the focus of the HCCH's work in the area has been on specific private international law issues arising from emerging technologies and applications in the digital economy, including DLT applications, such as:

- 'jurisdiction and choice of court (e.g., how to determine the competent court to resolve a dispute in relation to a crypto asset),
- applicable law and choice of law (e.g., what is the most appropriate connecting factor defining the law applicable to a transaction via blockchain)'.
- recognition and enforcement (e.g., how to enforce a foreign judicial decision in relation to a service regulated by a smart contract), and
- cross-border and cross-platform cooperation mechanisms (e.g., what cooperation frameworks are feasible and desirable to overcome challenges that the digital economy faces).'[72]

Specific private international challenges raised by 'digital and crypto currencies' as well as 'DLT and blockchain' are also under consideration by the HCCH as part of this work.[73] These issues were included in the programme of the HCCH CODIFI (Commercial, Digital and Financial Law Across Borders) Conference,

---

69 See HCCH, *op. cit.,* note 8; *HCCH, Developments with respect to PIL implications of the digital economy, including DLT*, Preliminary Document No 4 of November 2020, [https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf], Accessed 1 February 2023); HCCH, *Developments with respect to PIL Implications of the Digital Economy*, Prel. Doc. No 4 REV of January 2022, [https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f32dac.pdf], Accessed 1 February 2023; HCCH, *Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report*, [https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf], Accessed 1 February 2023.

70 See HCCH, Prel. Doc. No 4 of November 2020, *ibid.,* pars. 5-7; HCCH Prel. Doc. No 4 REV of January 2022, *ibid.,* pars. 4-7.

71 See HCCH, *About the HCCH,* [https://www.hcch.net/en/about], Accessed 1 February 2023.

72 See HCCH, Prel. Doc. No 4 of November 2020, *op. cit.,* note 69, par. 7; Prel. Doc. No 4 REV of January 2022, *op. cit.,* note 69, par. 8. See also Prel. Doc. 28 of February 2020, *op. cit.,* note 69, pars. 9-15.

73 See HCCH, Prel. Doc. No 4 REV of January 2022, *op. cit.,* note 69, pars. 13-17 and 29-31.

successfully held online in September 2022, under the Conference's digital economy thematic tracks.[74] The outcomes of the CODIFI Conference were published in the conference report in January 2023.[75] The report referred to the inherent cross-border element of the topics concerned in various parts and accordingly noted that considerations of private international law are crucial.[76] The report also highlighted, *inter alia*, that various private international law issues identified by experts at the Conference may benefit from potential future work in relation to jurisdiction, applicable law, choice of forum, party autonomy, recognition and enforcement, and international cooperation mechanisms.[77]

Against this background, the Permanent Bureau developed a number of joint initiatives for the consideration of the Council on General Affairs and Policy, one being the Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens.[78] This proposal built on one of the outcomes of the CODIFI Conference that several experts had agreed that 'work on private international law (PIL) relating to digital assets, specifically the determination of applicable law, is both timely and desirable'.[79] The proposal's purpose was accordingly 'to examine, jointly with UNIDROIT, the desirability of developing coordinated guidance and the feasibility of a normative framework on the law applicable to cross-border holdings and transfers of digital assets and tokens, covering relevant private law aspects'.[80] Starting with Principle 5 of the draft UNIDROIT Principles, this joint work was proposed to include:

- 'the applicable law in the absence of an explicit choice of law by the parties;
- weaker party protection in transactions relating to digital assets and tokens;
- connecting factors that would impact on the law applicable to cross-border holdings and transfers of digital assets and tokens; and

---

74 See HCCH, *The HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI),* [https://www.hcch.net/en/projects/post-convention-projects/hcch-codifi-conference], Accessed 1 February 2023. The videos of the sessions can be viewed at [https://www.youtube.com/playlist?list=PLL-3fQvUXrbUE0D2Oevr8VoAYUXIQ1AD-], Accessed 1 February 2023.

75 See HCCH, *Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report,* Prel. Doc. No 3A of January 2023, [https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf], Accessed 3 February 2023.

76 *Ibid.,* par. 13.

77 *Ibid.*, par. 5 and pp. 28-29.

78 See HCCH, Prel. Doc. No 3C of January 2023, *Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens*, [https://assets.hcch.net/docs/a91fd233-acf7-4c42-9aad-a426c4565068.pdf], Accessed 1 February 2023.

79 *Ibid.*, par. 2.

80 *Ibid.*, par. 3.

- the law applicable to linked assets'.[81]

The HCCH-UNIDROIT Joint Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens (HCCH-UNIDROIT Digital Assets and Tokens Joint Project) was approved by the HCCH Council on General Affairs and Policy in March 2023[82] and by the UNIDROIT Governing Council in May 2023.[83] The kick-off meeting of the Joint Project was held in June 2023 and, following a second meeting in autumn 2023, the HCCH Permanent Bureau will report the Council on General Affairs and Policy on the project results, including suggestions on the desirability and feasibility of continuing work on the topic through the establishment of a joint Experts' Group.[84]

As is seen, the HCCH has identified a number of private international law issues in the area, some of them being the core questions of private international law. However, internationality has not been among them although it is key to all the issues identified so far. It is interesting to note that HCCH did consider the question of internationality as part of its work on the law applicable to international credit transfers, which started in 1980s but not resulted in any legal instrument.[85]

4. CONCLUDING REMARKS

Internationality is a fundamental concept in private international law which defines the relevance and applicability of this area of law in a given situation. Although there is no agreement in private international law as to how internationality is to be ascertained for a transaction, relationship or situation and on which criteria, internationality is typically considered as a requirement to be satisfied for a private international law analysis. This suggests that for a cryptocurrency transfer to be subject to a private international law analysis, there needs to be an element which gives the transfer an international character. However, this also gives rise to

---

81 *Ibid.*, par. 18.

82 See HCCH, *Launch of the HCCH-UNIDROIT Digital Assets and Tokens Joint Project*, [https://www.hcch.net/en/news-archive/details/?varevent=913], Accessed 31 July 2023.

83 See further the Project Proposal as presented to the UNIDROIT Governing Council, UNIDROIT, *Item No. 6 on the agenda: Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens*, 2023, [https://www.unidroit.org/wp-content/uploads/2023/05/C.D.-102-12-Proposal-for-Joint-Work-HCCH-UNIDROIT.pdf], Accessed 31 July 2023.

84 See *Kick-off Meeting of the HCCH-UNIDROIT Digital Assets and Tokens Joint Project*, [https://www.hcch.net/en/news-archive/details/?varevent=921], Accessed 31 July 2023.

85 HCCH, *Note on the Problem of the Law Applicable to International Credit Transfers*, Preliminary Document No 1 of November 1991, drawn up by Michel Pelichet, pp. 63-65.

the question of if, and how, such an element will be ascertained in cryptocurrency transfers taking place within truly global systems underpinned by DLT.

Given that DLT-based systems have participants located in different jurisdictions and that the ledger in these systems exist potentially in many places in the world as it is distributed across the system participants, there is no doubt that cryptocurrency systems underpinned by DLT ordinarily involve a foreign element. Although this makes a case for an argument that all cryptocurrency transfers within DLT-based systems are international and therefore should be subject to a private international analysis, this may not be always desirable for different reasons. Cryptocurrencies are used in purely domestic situations, as well as international ones, in various contexts and therefore disputes arising from cryptocurrency transfers may not necessarily involve a foreign element beyond the global nature of the systems within which cryptocurrencies are transferred. In addition, private international law is a technical area of law which gives rise to complex questions of the determination of international jurisdiction and applicable law, particularly in relation to novel concepts like cryptocurrencies. It would be therefore a costly and time-consuming exercise to conduct a private international law analysis in all cases arising from cryptocurrency transfers irrespective of the nature of the dispute. These considerations suggest that, for a private international law analysis of cryptocurrency transfers within DLT-based systems, there is therefore a need for a criterion or criteria on the internationality.

However, the criteria, which are traditionally used in private international law and which derive from persons or places/locations concerned, have limited utility in the cryptocurrency context due to the use of DLT, disintermediation and pseudonymity in cryptocurrency systems. In cases where there is some degree of identification of the transacting parties, the test for internationality may be based on the location of the parties if this is known or identifiable, or the internationality of a cryptocurrency transfer may be subject to the internationality of the underlying relationship between the transacting parties. However, this is not an area where specific pre-set and precisely defined criteria or definition of internationality could satisfactorily work given the fast-evolving and developing nature of cryptocurrencies and the difficulties associated with the application of any criterion based on persons or places/locations to cryptocurrencies. Therefore, there needs to be some flexibility in the test of internationality for cryptocurrency transfers in DLT-based systems. Although it is not clear whether the UNIDROIT and the HCCH take a particular approach to internationality in the context of their current projects concerning digital assets and digital economy, including cryptocurrencies, and, if they do, what that approach is, internationality would be key to many questions they have identified to address in the area.

REFERENCES

BOOKS AND ARTICLES

1. Albornoz, M.; Gonzalez Martin, N., *Towards the uniform application of party autonomy for choice of law in international commercial contracts*, Journal of Private International Law, Vol. 12, No. 3, 2016, pp. 437-465
2. Ali, R.; Barrdear, J.; Clews, R.; Southgate, J., *Innovations in Payment Technologies and the Emerge of Digital Currencies,* Bank of England Quarterly Bulletin, Vol. 54, 2014, pp. 262-275
3. Collins, L., *Contractual Obligations- The ECC Preliminary Draft Convention on Private International Law*, International and Comparative Law Quarterly, Vol. 25, No.1, 1976, pp. 35-57
4. Cox, R.; Taylor, J., *Funds Transfer*, in: Brindle, M.; Cox, R. (eds.), *Law of Bank Payments*, Sweet & Maxwell, 2017
5. Delaume, G. R., *What is an International Contract? An American and a Gallic Dilemma*, International and Comparative Law Quarterly, Vol. 28, No.2, 1979, pp. 258-279
6. Garriga Suau, G., *Blockchain-based smart contracts and conflict rules for business-to-business operations*, *Revista Electrónica de Estudios Internacionales, Vol. 41, 2021, pp. 1-27*
7. Geva, B., *Banking in the Digital Age- Who is Afraid of Payment Disintermediation*, EBI Working Paper Series, No. 23, 2018
8. Geva, B., *The Law of Electronic Funds Transfers*, Matthew Bender, 1994
9. Hodson, D., *Cryptocurrency and the Family Courts – Some International Experiences*, Financial Remedies Journal, No. 1, 2023
10. Karageorgiou, S., *Electronic Funds Transfers: Technical & Legal Overview*, Thesis, University of London Queen Mary and Westfield College, 1990
11. Kraus, D.; Obrist, T.; Hari, O. (eds.), *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, Edward Elgar, Cheltenham/Northampton, 2019
12. Kronke, H., *Connecting Factors and Internationality in Conflict of Laws and Transnational Commercial Law*, in: *Boele-Woelki,* K.; *Einhorn,* T.; *Girsberger, D.; Symeonides, S. (eds.), Convergence and Divergence in Private International Law– Liber Amicorum Kurt Siehr*, Eleven International Publishing – Schulthess, The Hague– Zürich, 2010, pp. 57-70
13. Lando, O., *International Situations and Situations Involving a Choice between the laws of Different Legal Systems*, in: Lipstein, K. (ed), *Harmonization of private international law by the E.E.C*, Institute of Advanced Legal Studies, London, 1978
14. Lando, O., *The Conflict of Laws of Contracts: General Principles*, Recueil des Cours, Vol. 189, 1984
15. Lomnicka, E.; Hare, C. V. M, *Modern Banking Law*, 5th ed, OUP, Oxford, 2011
16. Lord Collins of Mapesbury *et al.*, *Dicey, Morris & Collins on the Conflict of Laws*, 15th ed, Sweet and Maxwell, 2014
17. Malek, A.; Odgers, J., *Paget's Law of Banking*, 14th ed, Lexis Nexis, 2014
18. Mills, A., *Party Autonomy in Private International Law*, CUP, Cambridge, 2018
19. Nakamoto S, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

20. Nomer, E., *Devletler Hususi Hukuku*, 21st ed., Beta, İstanbul, 2015
21. Nygh, P., *Autonomy in International Contracts*, OUP, Oxford, 1999
22. Ostendorf, P., *The choice of foreign law in (predominantly) domestic contracts and the controversial quest for a genuine international element: potential for future judicial conflicts between the UK and the EU?*, Journal of Private International Law, Vol. 17, No. 3, 2021, pp. 421-438
23. Proctor, C., *The Law and Practice of International Banking*, 2nd ed, OUP, Oxford, 2015
24. Rühl, G., *Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?* in Cappiello, B.; Carulo, G. (eds.), *Blockchain, Law and Governance*, Springer, 2021, pp. 159-180
25. Symeonides, S. C., *Codifying Choice of Law Around the World: An International Comparative Analysis,* OUP, Oxford, 2014
26. Tekinalp, G.; Uyanık, A., Çavuşoğlu, *Milletlerarası Özel Hukuk Bağlama Kuralları*, 12th ed, Vedat, İstanbul, 2016
27. von Hoffmann, B., *General Report on Contractual Obligations* in Lando, O.; von Hoffmann, B.; Siehr, K. (eds.), *European Private International Law of Obligations*, Tübingen, J.C.B. Mohr (Paul Siebeck), 1975
28. Weller, M., *Choice of court agreements under Brussels Ia and under the Hague Convention: Coherences and clashes*, Journal of Private International Law, Vol. 13, No. 1, 2017, pp. 91-129
29. Yüksel, B., *Choice of Law in Civil and Commercial Matters under Turkish Private International Law in Comparison with their Equivalents under the Rome I and Rome II Regulations,* in: Beaumont, P.; Yüksel, B. (eds.), *Turkish and EU Private International Law: A Comparison*, Istanbul, XII Levha, 2014
30. Yüksel, B., *Facilitating International Trade between Turkey and China by International Payments via Electronic Funds Transfer: Problems and Possible Solutions under the UNCITRAL Model Law on International Credit Transfers*, in: Yenidünya, C.; Erkan, M.; Asat, R. (eds.), Reopening the Silk Road in the Legal Dialogue Between Turkey and China, Adalet, Ankara, 2013
31. Yüksel, B., *Uluslararası Elektronik Fon Transferine Uygulanacak Hukuk*, XII Levha, 2018
32. Yüksel Ripley, B., *Cryptocurrency Transfers in Distributed Ledger Technology-Based Systems and Their Characterisation in Conflict of Laws* in: Borg-Barthet, J.; Trimmings, K.; Yüksel Ripley, B.; Živković, P. (eds.), *From Theory to Practice in Private International Law: Gedächtnisschrift for Professor Jonathan Fitchen*, Hart Publishing, Oxford, forthcoming
33. Yüksel Ripley, B.; Heindler, F., *The Law Applicable to Cryptoassets: What Policy Choices are ahead of us* in Bonomi, A.; Lehmann, M; Lalani S. (eds.), *Distributed Ledger Technologies and Private International Law*, Brill, forthcoming

EU LAW

1. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6

HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW

1. Convention on Choice of Court Agreements, 30 June 2005

2. Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, 5 July 2006
3. Convention on the Law Applicable to Contracts for the International Sale of Goods, 22 December 1986
4. HCCH, *About the* HCCH, [https://www.hcch.net/en/about], Accessed 1 February 2023
5. HCCH, Commentary of the HCCH 2015 Principles on Choice of Law in International Commercial Contracts, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=135], Accessed 1 February 2023
6. HCCH*, Developments with respect to PIL implications of the digital economy, including DLT*, Preliminary Document No 4 of November 2020, [https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf], Accessed 1 February 2023
7. HCCH, *Developments with respect to PIL Implications of the Digital Economy*, Prel. Doc. No 4 REV of January 2022, [https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f-32dac.pdf], Accessed 1 February 2023
8. HCCH, *Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report*, [https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf], Accessed 1 February 2023
9. HCCH, *Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report,* Prel. Doc. No 3A of January 2023, [https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf], Accessed 3 February 2023
10. HCCH, Launch of the HCCH-UNIDROIT Digital Assets and Tokens Joint Project, [https://www.hcch.net/en/news-archive/details/?varevent=913], Accessed 31 July 2023
11. HCCH, *Note on the Problem of the Law Applicable to International Credit Transfers*, Preliminary Document No 1 of November 1991
12. HCCH, *Prel. Doc. No 3C of January 2023*, *Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens*, [https://assets.hcch.net/docs/a91fd233-acf7-4c42-9aad-a426c4565068.pdf], Accessed 1 February 2023
13. HCCH, *Principles on Choice of Law in International Commercial Contracts*, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=135], Accessed 1 February 2023
14. HCCH, *Proposal for the Allocation of Resources to Follow Private International Law Implications relating to Developments in the Field of Distributed Ledger Technology*, in particular in relation to 'Financial Technology', Preliminary Document 28 February 2020, [https://assets.hcch.net/docs/f787749d-9512-4a9e-ad4a-cbc585bddd2e.pdf], Accessed 1 February 2023
15. HCCH, *The HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI),* [https://www.hcch.net/en/projects/post-convention-projects/hcch-codifi-conference], Accessed 1 February 2023. The videos of the sessions can be viewed at [https://www.youtube.com/playlist?list=PLL3fQvUXrbUE0D2Oevr8VoAYUXIQ1AD-], Accessed 1 February 2023
16. *Kick-off Meeting of the HCCH-UNIDROIT Digital Assets and Tokens Joint Project*, [https://www.hcch.net/en/news-archive/details/?varevent=921], Accessed 31 July 2023

UNCITRAL

1. de Caria, R., *A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities*, *Modernizing International Trade Law to Support Innovation and Sustainable Development,* UNCITRAL, 2017, [https://aperto.unito.it/retrieve/handle/2318/1632525/464608/R.%20de%20Caria%2c%20A%20Digital%20Revolution%20%282017%29.pdf], Accessed 1 February 2023
2. UNCITRAL, *Explanatory Note on the UNCITRAL Model Law on International Credit Transfers*, 1992, [https://uncitral.un.org/en/texts/payments/modellaw/credit_transfers], Accessed 1 February 2023
3. UNCITRAL, *Model Law on International Credit Transfers*, [https://uncitral.un.org/en/texts/payments/modellaw/credit_transfers], 1992, Accessed 1 February 2023
4. United Nations Commission on International Trade Law, *UNCITRAL Legal Guide on Electronic Funds Transfers*, 1987, [www.uncitral.org/pdf/english/texts/payments/transfers/LG_E-fundstransfer-e.pdf], Accessed 1 February 2023

UNIDROIT

1. UNIDROIT, *Digital Assets and Private Law- Public Consultation,* [https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/digital-assets-and-private-law-public-consultation], Accessed 1 February 2023
2. UNIDROIT, *Digital Assets and Private Law: Study LXXXII Digital Assets and Private Law Project,* [https://www.unidroit.org/work-in-progress/digital-assets-and-private-law], Accessed 1 February 2023
3. UNIDROIT, *Item No. 4 on the agenda: Adoption of Draft UNIDROIT Instruments (c) Principles on Digital Assets and Private Law*, 2023, [https://www.unidroit.org/wp-content/uploads/2023/04/C.D.-102-6-Principles-on-Digital-Assets-and-Private-Law.pdf], Accessed 31 July 2023
4. UNIDROIT, *Item No. 6 on the agenda: Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens*, 2023, [https://www.unidroit.org/wp-content/uploads/2023/05/C.D.-102-12-Proposal-for-Joint-Work-HCCH-UNIDROIT.pdf], Accessed 31 July 2023

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/834) as amended by the Jurisdiction, Judgments and Applicable Law (Amendment) (EU Exit) Regulations (SI 2020/1574)

REPORTS

1. Goode, R.; Kanda, H.; Kreuzer, K. with the assistance of Bernasconi, C., *Hague Securities Convention Explanatory Report*, HCCH, 2017

2. Hartley, T.; Dogauchi, M., *Explanatory Report of the Convention of 30 June 2005 on Choice of Court Agreements*, HCCH, [https://www.hcch.net/en/publications-and-studies/details4/?pid=3959&dtid=3]
3. von Mehren, A. T., *Explanatory Report of the Convention on the Law Applicable to Contracts for the International Sale of Goods*, HCCH, 1987
4. UK Cryptoassets Taskforce, *Final report*, 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf], Accessed 1 February 2023
5. UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts*, 2019, [https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf], Accessed 1 February 2023

WEBSITE REFERENCES

1. EAPIL Working Group on the Law Applicable to Digital Assets, *The position paper of the European Association of Private International Law (EAPIL) in response to the public consultation on the UNIDROIT Draft Principles and Commentary on Digital Assets and Private Law issues*, 2023, [https://eapil.org/wp-content/uploads/2023/03/EAPIL-WG-Digital-Assets-Position-paper-March-2022-Final.pdf], Accessed 20 March 2023
2. Yüksel, B.; Heindler, F., *Use of Blockchain Technology in Cross-Border Legal Cooperation under the Conventions of the Hague Conference on Private International Law (HCCH)*, Aberdeen Law School Blog, 2019. [https://www.abdn.ac.uk/law/blog/use-of-blockchain-technology-in-crossborder-legal-cooperation-under-the-conventions-of-the-hague-conference-on-private-international-law-hcch/], Accessed 1 February 2023
3. Yüksel Ripley, B.; MacPherson, A.; Poesen, M.; Albargan, A.; Xuan Tung, L., *The response of the Centre for Commercial Law at the University of Aberdeen to the UNIDROIT Digital Assets and Private Law Consultation*, 2023, [https://www.abdn.ac.uk/law/research/centre-for-commercial-law/public-policy-stakeholder-engagement-1109.php], Accessed 21 February 2023

UDK 342.7:004.8
Original scientific paper

ALGORITHMIC DISCRIMINATION: A BLUEPRINT FOR A LEGAL ANALYSIS*

Patricia Živković, PhD, Lecturer
University of Aberdeen, School of Law
High Street, Aberdeen, AB24 3UB, United Kingdom
patricia.zivkovic@abdn.ac.uk

Rossana Ducato, PhD, Senior Lecturer
University of Aberdeen, School of Law
High Street, Aberdeen, AB24 3UB, United Kingdom
rossana.ducato@abdn.ac.uk

ABSTRACT

The paper aims at providing an overview of the issues raised by algorithmic discrimination, and the key contributions proposed in the literature to address them. It is intended to be used as a starting point for those interested in approaching the topic for the first time or as a syllabus for the students taking the Erasmus+ Strategic Partnership MOOC "Time to Become Digital in Law".

First, the contribution will outline what algorithms are and what we consider algorithmic bias and what are its causes. Second, it will investigate the ethical and social implications of algorithmic bias. Then, the paper will focus on how existing laws and regulations can be applied to algorithmic discrimination. This contribution will focus in particular on the two branches of law that have been identified in the literature as the most relevant in this context: anti-discrimination law and data protection law. The work will outline their potentialities and limitations, presenting some proposals advanced in the literature to fill the new and emerging gaps of protection.

***Keywords*:** *Artificial Intelligence, Bias, Algorithmic discrimination, Anti-discrimination law, Data Protection Law*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

Algorithmic bias is more and more commonly discussed in academic circles, and it necessitates perspectives from different disciplines, such as computing science, psychology, ethics, sociology, law, and others. It is a phenomenon that is by its nature multidisciplinary and interdisciplinary, and for that reason, it is also difficult to properly understand and regulate. At the heart of our paper lies the general concern of the possibility to replicate biased attitudes held by humans into machines and new discriminatory machine-generated practices. To provide a holistic view of the topic, one needs to understand the sources of automation bias, the ethical and social implications of such bias, and the current protection offered by the existing legal framework.

This is what we provided in the Massive Open Online Courses (MOOC), "Algorithmic discrimination: a blue-print for a legal analysis", that we designed for the project "Time to Become Digital in Law" (https://www.pravos.unios.hr/digin-law/), co-funded by the Erasmus Plus Programme of the European Union. This paper follows the structure of the MOOC, and it serves as a basic introduction to key legal issues raised by algorithmic discriminatory practices and the ways to counteract them. It is intended to be used as a starting point for those interested in approaching the topic for the first time or as a syllabus for the students taking the MOOC.

The paper starts with an explanation of what algorithms are and what we consider algorithmic bias and what are its causes (Section 2). This is a fundamental point to understand before we investigate the ethical and social implications of algorithmic bias (Section 3). We will stress in this part the difficult role of law to capture these implications timely and to follow rapid technological development. The paper will then focus on how existing laws and regulations can be applied to algorithmic discrimination. This contribution will focus in particular on the two branches of law that have been identified in the literature as the most relevant in this context: anti-discrimination law (Section 4) and data protection law (Section 5). We will outline their potentialities and limitations, presenting some proposals advanced in the literature to fill the gaps of protection.

2. ALGORITHMS AND AUTOMATION BIAS EXPLAINED

An algorithm is an abstract, formalised description of a computational procedure that can be used, *inter alias*, for automated decision-making.[1] Such a decision-

[1] Zuiderveen Borgesius, F., *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*, Council of Europe, 2018, Strasbourg, p. 11.

making process can be fully automated or partly automated.[2] These forms of decision-making will depend on whether there is a human in the loop and to what extent: in the case of a fully automated algorithm, the decision is made entirely by an algorithm; whereas with partly automated algorithms humans are making the final decision in the end.[3] However, both partly and fully automatic decision-making may lead to discrimination. Hence, in this paper, we refer to "algorithmic discrimination" whether the discriminatory practice is performed via solely automated decision-making or support systems.

In general terms, algorithmic discrimination usually results from the lack of time, context, skills, and knowledge to assess the adequacy of automatically made decisions.[4] In the past two decades, this phenomenon has attracted the attention of academics and practitioners in law, computing science, psychology, and other disciplines and both state and corporate use of these machines has been flagged as an issue to be approached with caution and proper investigation.[5] To provide a broader understanding of this phenomenon, we will explore in this Section the discrimination risks involved in algorithmic decision-making and the fields most affected by those risks.

Algorithmic discrimination is complex and sensitive topic when it comes to machine learning. Machine learning systems are the most well-known artificial intelligence ("AI") systems.[6] These systems, instead of being given predetermined sets of solutions, are set a task and provided with training data, based on which they make decisions.[7] They will be at the heart of this paper, and the notions of "AI-based systems" and "machine learning" will for that purpose be used interchangeably.

AI-based systems have already been widely integrated into today's society and are used by all of us. The newly proposed legislations and regulations are, among

---

2 *Ibid.*

3 *Ibid.*

4 *Ibid.*

5 Kearns, M.; Aaron Roth, A., *The Ethical Algorithm: The Science of Socially Aware Algorithm Design*, Oxford University Press, Oxford, 2020; Broussard, M., *Artificial Unintelligence: How Computers Misunderstand the World*, First MIT Press paperback edition, The MIT Press, 2019; Zuiderveen Borgesius, *op. cit.*, note 1; O'Neil, C., *Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, 2018; Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, First Trade Paperback Edition, Public Affairs, 2020; Webb, A., *The Big Nine*, Ingram Publisher Services US, 2019.The MIT Press 2019

6 Zuiderveen Borgesius, *op. cit.*, note 1, p. 13.

7 *Ibid.*

other reasons, based on the need to scrutinise the systems and prevent any integration of discriminatory practices and or results in their use.

One may naturally start with a question: How can AI lead to discrimination? To answer that, we need to get acquainted with the term "black box". The black box phenomenon in relation to AI means that it is often unclear to human beings how the AI system makes decisions, and this makes it difficult to assess whether there is any discrimination.[8]

Barocas and Selbst list six technical examples, where the sources of potential discrimination are discernible, although with some effort, and hence, the discriminatory practices and results stemming from the use of an AI-based system can be understood from their roots:

1. Defining the "target variable" and "class labels",
2. Training data: labelling examples,
3. Training data: data collection,
4. Feature selection,
5. Proxies, and
6. Intentional discrimination.[9]

The first example of an AI system leading to discrimination relates to the notions and defining process of target variables and class labels. The target variable is an outcome of interest, or in other words, the outcome the user wishes to achieve by using the system.[10] Class labels represent values relevant to the target variable which are mutually exclusive.[11] To showcase how defining the target variable and class labels can lead to discrimination, we can use an example of almost any performance assessment AI system. If we want to assess the performance of employees, we would need to define what a "good" or "desirable" employee is, and what a "bad" employee is, and these would be class labels.[12] A desirable employee could then be defined as an employee who is rarely or never late, and an undesirable or bad employee could be defined as someone who is often late.[13] The potential for discrimination lies in these definitions as the reason for being late to work can stem from the social context. For example, people who are on average poorer may

---

8 *Ibid.*, p. 15.

9 Barocas, S.; Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, Vol. 104, No. 3, 2016, p. 671; as reported in Zuiderveen Borgesius, *op. cit.*, note 1, pp. 15–23.

10 Barocas; Selbst, *op. cit.*, note 9, p. 678; Zuiderveen Borgesius, *op. cit.*, note 1, p. 16.

11 Zuiderveen Borgesius, *op. cit.*, note 1. p. 16.

12 Barocas; Selbst, *op. cit.*, note 9, p. 678; Zuiderveen Borgesius, *op. cit.*, note 1, pp. 16–17.

13 Zuiderveen Borgesius, *op. cit.*, note 1, pp. 16–17.

live farther from their work, and this social circumstance makes them more likely to be late.[14] Hence, the system would potentially discriminate against such employees when assessing their work.

The next two examples of an AI system that may lead to discrimination are when the system learns from discriminatory training data. The AI system can either be trained on biased data, or it can learn from a biased sample.[15] In other words, we can say that the old principle "bias in, bias out" is visible in these situations.[16]

Algorithmic bias can result from the use of biased training data in those situations when the training data is collected in the past and does not reflect today's ethical and moral values, which are transposed to anti-discrimination law. For example, if appointment to positions or jobs was previously not allowed to women, or they were discriminated against in the past, and we train the AI system based on historical data, the discriminatory effect will be replicated.[17]

Similarly to the previous example, an AI system may lead to discrimination when the system learns from training data that is collected through a biased sampling procedure.[18] For example, to train a system that is set to predict crime, the data was collected by the police who focused their attention on certain ethnic groups and certain neighbourhoods.[19] Depending on who lives in those neighbourhoods, the AI system will provide biased results against those groups of people.

The fourth example of an AI system that can lead to discrimination relates to feature selection by the user of the system. Namely, users of the AI system may be required to set the features they want to be captured through processing and lead to the target variable, and these need to be simplified for the system to capture them in data.[20] The features, i.e. categories of data, to be analysed by the system do not need to be directly discriminatory, and usually, they are not. However, that does not mean they will not produce discriminatory results. For example, if an AI system is handling many job applications and is tasked to shortlist applicants who have a degree from one of the highest-ranked universities, this could lead to

14 *Ibid,* p. 17.

15 Barocas; Selbst, *op. cit.*, note 9, p. 681; Zuiderveen Borgesius, *op. cit.*, note 1, pp. 17–19.

16 Selmi, M., *Algorithms, Discrimination and the Law*, Ohio State Law Journal, Vol. 82, No. 4, 2021.

17 Similarly in Barocas; Selbst, *op. cit.*, note 9, p. 682.

18 Zuiderveen Borgesius, *op. cit.*, note 1, pp. 18–19.

19 *Ibid.*, p. 19.

20 Barocas; Selbst, *op. cit.*, note 9, p. 688; Zuiderveen Borgesius, *op. cit.*, note 1, p. 20.

discriminatory effects against those that had no economic means to access such education.[21]

The fifth example of an AI-based system that leads to discrimination relates to proxies, which are criteria that are genuinely relevant in marking rational and non-discriminatory decisions, but they indirectly link to biased attitudes.[22] For example, if one uses an AI-based application for approving loan applications, the target variable is to approve loans to those people who will not likely default, and through training, the machine learns that people from certain postcodes default more.[23] Despite being non-discriminatory at its face value, this criterium may lead to a discriminatory effect as it may act as a proxy for racial origin.[24] In other words, a protected characteristic may be encoded in other data, as in this case racial origin is encoded in a postcode.

Finally, the last example of an AI system according to Barocas and Selbst that can lead to discrimination encompasses a situation in which the discrimination is intentional (despite being masked as one of the above examples).[25] For example, if the users of the system have set the task for the system to identify women based on shopping behaviour to market other products to them and adjust the prices.[26]

Based on the outline of the issues presented in this section, one can conclude that it is important to understand that discrimination risks can be hidden and reproduced in different ways and that education on discrimination and a proper understanding of machine learning is crucial for the prevention of such results. There are fields in which AI brings the most discrimination risks and these require special attention in order to provide an adequate legal framework. An observation of not only the technical causes of algorithmic discrimination, but also the ethical and social implications of such applications is a step towards such a legal framework. Such implications are addressed in the next section of this paper.

3. ETHICAL AND SOCIAL IMPLICATIONS OF AI APPLICATIONS

This section will be divided into three parts. First, the components of trustworthy AI will be briefly introduced, followed by a presentation of the definition and

---

21 Barocas; Selbst, *op. cit.*, note 9, p. 688; Zuiderveen Borgesius, *op. cit.*, note 1, p. 20.

22 Barocas; Selbst, *op. cit.*, note 9, p. 691; Zuiderveen Borgesius, *op. cit.*, note 1, p. 21.

23 Zuiderveen Borgesius, *op. cit.*, note 1, p. 21.

24 *Ibid.*

25 Barocas; Selbst, *op. cit.*, note 9, p. 692; Zuiderveen Borgesius, *op. cit.*, note 1, p. 22.

26 Zuiderveen Borgesius, *op. cit.*, note 1, pp. 22–23.

scope of ethical AI and robust AI and the social implications of the lack of such attributes (Section A). After that, the paper will address the phenomenon of ethics washing, which is developed to create and preserve an image of ethical behaviour in the corporate field of Big Tech (Section B). Finally, from the sociological stance, a parallel is drawn between the (unconscious) biases held by programmers and biased programmes as a result (Section C).

A. Trustworthy AI and its social implications

EU guidelines defined three components of Trustworthy AI in 2019.[27] Ethics plays a crucial role in this definition.

Trustworthy AI has three components, which should be met throughout the system's entire life cycle:

1. it should be lawful, complying with all applicable laws and regulations;
2. it should be ethical, ensuring adherence to ethical principles and values; and
3. it should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.[28]

Whereas the lawfulness of AI will be the topic of Sections 4 and 5 in this paper from the stance of anti-discrimination and data protection laws, we will focus on exploring ethical and robust AI in this part.

Achieving Trustworthy AI requires not only compliance with the law; as a matter of fact, laws are not always up to speed with technological developments.[29] Trustworthy AI inevitably requires also compliance with ethical principles and values, and a warranty of the robustness of such a system to prevent any harm to citizens.

There is some overlap between legal and ethical standards. The fundamental rights families are particularly suitable to cover AI systems among the broad range of indivisible rights outlined in international human rights legislation, the EU Treaties, and the EU Charter, making these rights legally enforceable.[30] However, even after adherence to fundamental rights is made legally enforceable, considering ethical norms can help us comprehend how the creation, application, and use of AI systems may conflict with these rights and the values that underpin them.[31] Also, as it

---

27 High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, Brussels, 2019.

28 *Ibid.*, p. 5.

29 *Ibid.*

30 *Ibid.*, p. 10.

31 *Ibid.*

will be shown in the next two sections, ethical consideration can impact the policymakers' and legislators thinking when it comes to the regulation of technology.

Concerns about human dignity (or whether AI systems should unjustifiably subordinate, coerce, deceive, manipulate, condition, or herd humans), the principle of prevention to harm (where special attention is being paid to situations where AI systems can cause or aggravate negative impacts due to asymmetries of power or information), the principle of fairness (which is ensuring equal and just distribution of resources), and the principle of explicability (which means that processes need to be transparent and explainable) are the most crucial ethical considerations to be made.[32]

It is important to remember that implementing all the Trustworthy AI principles must be done throughout the system's life cycle. This requires a constant reassessment of such implementation and redesign of the legal framework when needed.

B. Ethics washing

The development of advisory boards, in-house moral philosophers, a focus on human design, and sponsoring "fair" machine learning are just a few of the corporations' attempts to create ethical products that have been made during the past few decades by major tech companies.[33] These initiatives can sometimes be used as a tool for ethics washing because they are not put in place for a good motive, and allow businesses to cite ethics as a legitimate pretext to explain deregulation, self-regulation, or market-based governance.[34]

Bietti warns that, in practice, these advisory councils or in-house moral philosophers have little power to shape internal company policies and that the corporations overstep the focus on human design – e.g. nudging users to reduce time spent on apps – instead of tackling the risks inherent in the existence of the products themselves.[35] What is important to notice is that the use of ethical language *per se* is not ethical washing, however, the misuse and instrumentalization of it for self-regulation and profit is.[36]

At least three possible arguments can be raised against initiatives that use ethical language and self-regulation for internal purposes. The proper application of mor-

---

32 *Ibid.*, pp. 12–13.

33 Elettra, B., *From Ethics Washing to Ethics Bashing: A View on Tech Ethics from Within Moral Philosophy*, 2021, Available at SSRN: [https://ssrn.com/abstract=3914119].

34 *Ibid.*

35 *Ibid.*

36 *Ibid.*

al philosophy can help resolve these. First, choices made by corporate AI ethical committees are constrained internally, subject to high management approval, and reliant on company funding.[37] As a result, when correctly implemented, moral philosophy can guide internal AI ethics committees toward advancing society.[38] Second, if practising moral philosophy is done for financial gain, employer satisfaction, or to earn recognition, it no longer maintains its intrinsic moral significance.[39] As a result, the right application of moral philosophy can guide the pursuit of justice and trust as well as the welfare of society.[40] Third, ethics rhetoric may encourage and support a constrained view of the potential for regulatory reform and stifle discussion.[41] Thus, by empowering activists and fostering social dialogue, the right application of moral philosophy improves society.[42]

Besides the better attempts at implementing the moral philosophy within corporations, and in that way indirectly into programmers' actions, another approach is also to implement these views through training the programmers directly. This is what the next Section will address.

C. Biased programmers or biased data

Two main theories explain most cases of bias in AI systems: the biased training data theory and the biased programmers theory.[43] It is sometimes difficult to distinguish the most contributing source to bias in AI systems.

As explained in the previous section, machine learning applications are often developed using historical data about outcomes, data coming from it would reflect and perpetuate any bias in the real world. The very fact that these were the datasets commonly used, makes it very hard to quantify the extent of this problem.

The second theory emphasizes another factor: biased programmers.[44] The community of programmers developing algorithms is highly non-representative and may exhibit biases that are passed onto the algorithms they write.[45] Some studies, however, found little effect of altering programmer demographics or from program-

37 *Ibid.*

38 *Ibid.*

39 *Ibid.*

40 *Ibid.*

41 *Ibid.*

42 *Ibid.*

43 Cowgill, B. et al, *Biased Programmers? Or Biased Data? A Field Experiment in Operationalizing AI Ethics*, in: Proceedings of the 21st ACM Conference on Economics and Computation, 2020.

44 *Ibid.*

45 *Ibid.*

mers who score worse on psychology measures of implicit bias.[46] This strongly suggests that organizations should strive to ensure data (e)quality, i.e. exert efforts to increase their data reliability and inclusivity. Issuing regular non-technical reminders to programmers about biases would also address the issue at the personal level, just as regular technical education on how to eliminate these biases in the development would do the same at the professional level.[47]

What was discussed so far deals with the preventive methods for algorithmic bias, but until we reach the stage of the utopian seamless prevention of discrimination, we need to look at the available legal framework for the resolution of these issues in practice. That is what Sections 4 and 5 will explain.

4. ALGORITHMIC DISCRIMINATION AND THE ANTI-DISCRIMINATION LEGAL FRAMEWORK

Non-discrimination and data protection law are among the legal areas, identified in the literature, that can offer the most comprehensive set of tools to address the risks to fundamental rights and freedoms caused by algorithmic discrimination.

While these frameworks can respond to some of the challenges outlined in Section 2, several issues remain open and need to be addressed from a *de lege lata* and *de lege ferenda* perspective. To this end, the paper will outline some of the key proposals that have been advanced by scholars to improve the *status quo*.

In this Section, we will deal with the anti-discrimination legal framework and move to data protection law in Section 5.

Non-discrimination is one of the fundamental principles in the European legal context, and it is recognised in several legal instruments at the national (constitutions and national laws), international,[48] and European levels.[49] The principle of

---

46 *Ibid.*

47 *Ibid.*

48 See, for instance, Art. 14 of the Convention for the protection of human rights and fundamental freedoms (ECHR), which prohibits discrimination based on any ground "such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".

49 At the EU level the principle of non-discrimination is enshrined in both primary (e.g. Art. 2 TEU; Arts. 10, 18, and 45 TFUE; Arts. 10 and 21 of the Charter of fundamental rights of the EU) and secondary law (Council Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation [2000] OJ L303/2000, Council Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/2000, Council Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L373/2004, and Di-

non-discrimination essentially entails that everyone shall have equal chances to access to opportunities in society.[50]

The existing legal framework can protect us against various forms of discrimination. For instance, a rule or a practice cannot lead to treating a person in a less favourable way than others in a similar situation because of a characteristic they possess (direct discrimination); neither a neutral provision – virtually applicable to all – can lead to disadvantage a protected person or group in practice (indirect discrimination).

Anti-discrimination law can also protect those persons that are discriminated against because they are associated with a protected group, even if they are not part of it (discrimination by association).[51]

Finally, the legal protection against multiple and intersectional discrimination can be particularly helpful in the context at stake, where algorithms differentiate people based on a number of characteristics and where the discrimination might not exclusively depend on one of them. Multiple discrimination occurs when someone is treated less favourably because of the sum or the sequence of different protected grounds (e.g. a lesbian might be discriminated against because she is a woman and gay).[52] There is intersectional discrimination when the interplay of different protected grounds generates a discriminatory effect that is qualitatively different from either ground taken in isolation. Friedman explains that:

"black women may experience discrimination in a way which is qualitatively different from either white women or black men. Black women share some experiences in common with both white women and black men, but they also differ in important respects. Thus while white women may be the victims of sex discrimination, they may also be the beneficiaries and even the perpetrators of racism. Conversely, black men may experience racism but be the beneficiaries and perpetrators of sexism."[53]

---

rective 2006/54/EC of the European Parliament and of the Council on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L204/2006).

50 European Union Agency for Fundamental Rights, *Handbook on European Non-Discrimination Law*, Publications Office of the EU, Luxembourg, 2018, p. 42.

51 This concept can be applied both in cases of direct and indirect discrimination.

52 European Union Agency for Fundamental Rights, *op. cit.*, note 50.

53 Fredman, S., *Intersectional Discrimination in EU Gender Equality and Non-Discrimination Law*, European Commission, Brussels, 2016, p. 7.

This framework can offer a series of tools also when applied in the context of algorithmic discrimination.

For instance, the prohibition of direct discrimination can cover situations where the algorithm bases the decision on a protected ground. However, according to several authors, direct discrimination might be relatively rare in practice.[54] In most cases, an algorithm can treat an individual less favourably based on correlations with a protected ground and not based on the protected ground itself.

Indirect discrimination could offer more grip to address this latter case, but only to a certain extent. Indirect discrimination is an open-ended clause and might be challenging to prove: it has to be verified on a case-by-case basis if a neutral rule impacts a protected category, and the victim should prove, at least, *prima facie* discrimination, usually through statistical evidence.[55] Moreover, a claim of indirect discrimination can be rebutted if the perpetrator has an objective justification (i.e. the differential treatment pursues a legitimate aim and is proportionate).[56]

More generally, it has been pointed out in the literature that anti-discrimination law protection is very much sectorial and covers only a limited number of grounds.[57] If someone is treated less favourably than another one in a similar situation, but the situation cannot fall within one of the protected grounds enumerated in the law, the victim will not be protected.

This shortcoming is particularly relevant in the context of inferential analytics, where data mining activities could identify new high-risk categories or reaffirms structural inequalities that are different from the protected characteristics that the Legislator considered a few years ago. People can be treated unjustly due to low

---

54 Zuiderveen Borgesius, *op. cit.*, note 1; Wachter, S., *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, Berkeley Tech. LJ, Vol. 35, No. 2, 2020, p. 367; Xenidis, R., *Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience*, Maastricht Journal of European and Comparative Law, Vol. 27, No. 6, 2021, p. 736. *Contra*, Adams-Prassl, J.; Binns, R.; Kelly-Lyth, A., *Directly Discriminatory Algorithms*, The Modern Law Review, Vol. 86, No. 1, 2023, p. 144. Building on the legal rationale of the distinction between direct and indirect discrimination and a through analysis of the case law, Prassl and others argue that the role of direct discrimination is more relevant than generally assumed in the legal discourse, and it could cover some cases of proxy discrimination and sampling bias.

55 Zuiderveen Borgesius, *op. cit.*, note 1.

56 As noted by Prassl and others, when the predictivity of an algorithm is high, this element can be used to support the proportionality claim. The problem, highlighted in the literature, is that an algorithm can be fed with a biased dataset, and if a predictive model is deployed, this latter can reinforce the existing stereotypes and create a risk of self-justifying feedback loops. Adams-Prassl; Binns; Kelly-Lyth, *op. cit.*, note 54.

57 Zuiderveen Borgesius, *op. cit.*, note 1; Wachter, *op. cit.*, note 54; Xenidis, *op. cit.*, note 54.

income, financial difficulties, or degree of education.[58] However, since these are not "protected grounds" under the EU legal framework - nor will it always be possible to demonstrate statistically the relation between the inference drawn by the algorithm and a protected group – the current anti-discrimination framework might be toothless.

Another open challenge of algorithmic discrimination refers to the well-known issue of the lack of transparency of such systems. Profiling is often obscure and the victims of discrimination might not necessarily be aware of how they have been classified by the algorithm and what are the consequences of the correlations made.[59] Indeed, machine learning algorithms are often "black boxes": it might be difficult to understand the logic behind the automated decision system because of the complexity of the algorithm. Algorithms can be black boxes due to legal constraints as well.[60] Many commercial providers often oppose trade secret protection to avoid the disclosure of the parameters of the algorithm. Moreover, profiling is a dynamic activity. Hence, the classification might evolve, uses other variables, and find new correlations and patterns.[61]

All these elements can have an impact in terms of access to justice. First, due to the black box problem and the dynamicity of profiling, it might be difficult for a potential victim even to find that they have been discriminated against.[62] Moreover, if the processing is opaque, the explanation unintelligible, and information cannot be disclosed, it is challenging to provide evidence of the discrimination (or the lack thereof).[63]

As for multiple and intersectional discrimination, they could overcome some of the issues raised by algorithmic discrimination. The automated decision often relies on a combination of factors and characteristics (it is well-known the case voiced by the MIT researchers, Joy Buolamwini and Timnit Gebru, who discovered that darker-skinned women are the group that facial recognition algorithms

58 Zuiderveen Borgesius, *op. cit.*, note 1; Wachter, *op. cit.*, note 54; Xenidis, *op. cit.*, note 54."

59 Zuiderveen Borgesius, *op. cit.*, note 1. *Wachter, S., The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Anti-Discrimination Law*, Tulane Law Review, Vol. 97, No. 2, 2022.

60 Malgieri, G. *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*, International Data Privacy Law, Vol. 6, No. 2, 2016, p. 102; Wachter, S.; Mittelstadt, B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. L. Rev., No. 2, 2019, p. 494.

61 Wachter, *op. cit.*, note 59.

62 Zuiderveen Borgesius, *op. cit.*, note 1); Wachter; Mittelstadt, *op. cit.*, note 60.

63 Zuiderveen Borgesius, *op. cit.*, note 1; Adams-Prassl; Binns; Kelly-Lyth, *op. cit.*, note 54.

most frequently misclassify).[64] However, multiple and intersectional are not expressly recognised in the law[65] or the case law of the CJEU.[66]

To fill the current gaps in protection, several scholars have suggested broadening the scope of anti-discrimination law because it does not perfectly capture the new risks posed by algorithmic decision-making systems.[67]

The expansion of the scope of anti-discrimination protection law could happen *de lege lata.* Xenidis, for instance, has argued for a purposive interpretation of key crucial concepts, such as the notion of intersectional discrimination.[68] The latter could alleviate the burden of proof of *prima facie* discrimination in the algorithmic context, but it has not been expressly recognised by the CJEU.[69] However, according to the author, such restrictive interpretation is not absolute: she reads some encouraging signs in the case law of the CJEU[70] and in the opinion of the Advocates General (in the case Parris and Léger)[71], where the concept of multiple discrimination could open the way to the recognition of intersectional discrimination as well.[72]

Along the same lines, she contends that a contextual and expansive interpretation of the protected grounds in EU anti-discrimination law is still viable. Despite the sectorial approach recognised in the Directive, the content of the grounds is not expressly defined in the law. Hence, a broad interpretation of these grounds will contribute to making EU equality law more effective because it will protect individuals against the new types of discrimination based on the patterns and correlations identified by algorithms.[73]

---

64 Buolamwini, J.; Gebru, T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in: Proceedings of Machine Learning Research, No. 81, Conference on fairness, accountability and transparency (PMLR 2018), 2018. The case is presented as an example of intersectional discrimination by Xenidis, *op. cit.*, note 54.

65 There is only a brief mention to multiple discrimination in the recitals of Directive 2000/43/EC (Recital 14) and 2000/78/EC (Recital 3).

66 Xenidis, *op. cit.*, note 54.

67 Zuiderveen Borgesius, *op. cit.*, note 1; Wachter, *op. cit.*, note 54; Xenidis, *op. cit.*, note 54; Adams-Prassl; Binns; Kelly-Lyth, *op. cit.*, note 54.

68 Xenidis, *op. cit.*, note 54.

69 *Ibid.*

70 Referring to Case C-152/11 *Johann Odar v Baxter Deutschland GmbH* [2012] ECLI:EU:C:2012:772.

71 Respectively, Case C-528/13 *Geoffrey Léger v Ministre des Affaires sociales, de la Santé et des Droits des femmes and Etablissement français du sang* [2014] ECLI:EU:C:2014:2112, Opinion of AG Mengozzi, and Case C-443/15 *David L. Parris v Trinity College Dublin and Others* [2016] ECLI:EU:C:2016:493, Opinion of AG Kokott.

72 Xenidis, *op. cit.*, note 54, pp. 743-744.

73 *Ibid.*, pp. 750-751.

As we have already pointed out, algorithmic discrimination can affect individuals even not relying on traditional protected grounds. According to Xenidis, the open-ended clause of Art. 21 of the Charter of fundamental rights and the principle of non-discrimination are interesting paths to explore, as they might provide enough flexibilities to address the new situations of harm.[74]

There are, however, challenges in this kind of approach, because the CJEU has been reluctant so far to expand the list of protected grounds. Given this premise, some authors called for a different hermeneutic approach. For instance, Wachter elaborated a new theory of harm that could close the gaps in protection.[75] She demonstrated that the legal rationale and the traditional categories of anti-discrimination law do not match the logic of algorithms. For instance, people can now be discriminated against based on non-protected features (because they are dog owners or video gamers), or characteristics that cannot be meaningfully caught by an individual (e.g. pixels in a picture).

However, such groups can experience the same harm as traditionally protected categories: ultimately, they are not given an equal opportunity to exercise their rights and freedoms, as well as to access goods to further their aims in life.[76]

Wachter notes that AI creates groups with "immutable" characteristics that the individual cannot control. This is what she calls artificial immutability. Such artificial immutability relies on five conditions: opacity (individuals do not know how they have been classified, or what the consequences are of that classification), vagueness (the individual cannot make meaningful decisions because they do not have transparent information), instability (the criteria are dynamic, they can change over time, so it is very difficult to rely on them), involuntariness and invisibility (the inputs processed by the algorithm are not self-evidently meaningful to people), and lack of social concept (the characteristics used by algorithms do not always find a functional equivalent concept in human language).[77]

This proposal has the merit to address the most subtle and invisible forms of algorithmic discrimination, identifying the new "protected grounds" in the attributes that are not under our control.

---

74 *Ibid.* pp. 755-757.

75 Wachter, *op. cit.*, note 59.

76 *Ibid.*

77 Wachter, *op. cit.*, note 59, pp. 43-45.

5. ALGORITHMIC DISCRIMINATION AND THE DATA PROTECTION FRAMEWORK

The data protection framework can offer a few valid tools that can complement the protection granted by anti-discrimination law.

For instance, the fundamental principles and the procedural guarantees laid down in the European framework, such as the Modernised Convention 108[78] and the General Data Protection Regulation (GDPR)[79], can offer a net of protection against those negative/discriminatory consequences suffered by individuals, whether the decision is fully or partially automated.

The data protection fundamental principles, in particular, the principles of lawfulness, fairness, transparency and accuracy require that processing should respect the rights and fundamental freedoms of individuals. Individuals should be informed in a clear and transparent way about how their data are processed by the machine, what the risks for them are, and what the implications are.[80] The accuracy principle should protect them against profiling misclassifications.[81]

Important data subjects' rights correspond to these principles. For instance, individuals enjoy the right to be informed about the key aspects of the processing – including its risks - in a timely and meaningful way (Arts. 12-14 GDPR). This can represent an important tool to counteract the black box problem because a data subject shall be informed about the existence of the automated decision-making process and receive meaningful information about the logic involved.[82]

---

78 Council of Europe, *Modernised Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 18 May 2018 (Modernised Convention 108).

79 Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L119/2016.

80 Zuiderveen Borgesius, *op. cit.*, note 1.

81 Wachter, *op. cit.*, note 54.

82 Kaminski, M. E., *The Right to Explanation, Explained*, in: Sandeen, S. K.; Rademacher, C.; Ohly, A. (eds.), Research Handbook on Information Law and Governance, Edward Elgar Publishing, Cheltenham, 2021, p. 278.or AI. The EU's General Data Protection Regulation (GDPR Although the existence and precise boundaries of the "right to explanation" has been challenged in the literature. See, Goodman, B.; Flaxman, S., *EU Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, AI Magazine, Vol. 38, No. 3, 2017; Wachter, S.; Mittelstadt, B.; Floridi, L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, Vol. 7, No. 2, 2017, p. 76; Malgieri, G.; Comandé, G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law, Vol. 7, No. 4, 2017; Edwards, L.; Veale, M., *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, Duke L. & Tech. Rev., Vol. 16, No. 1, 2017, p. 18; Selbst, A.; Powles, J., *Meaningful Information" and the Right to Explanation*, in: Proceedings of the 1st Conference on Fairness, Accountability and Transparency (PMLR 2018), Vol. 81, 2018.

The right to access (Art. 15 GDPR) can be used to verify whether someone is processing our data and discover if we are subject to automated decisions. Hence, it could be a tool to investigate potential cases of discrimination. If an individual has been misclassified, they can ask for the rectification of information (Art. 16 GDPR), etc.

A higher level of protection is recognized for the so-called "sensitive data". This category includes data that bear a high risk of discrimination for individuals, namely "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Art. 9 GDPR and Art. 6 Modernised Convention 108).[83]

Supervisory authorities can also play a fundamental procedural role in fighting algorithmic discrimination.[84] They are independent bodies that have the task to monitor the correct application of the GDPR. They have investigative powers, can perform an audit of the algorithm, and require the necessary documentation to see how it works in practice. Data Protection Authorities must also be consulted depending on the outcome of the Data Protection Impact Assessment (DPIA) performed by the controller.

The DPIA is a comprehensive analysis of the processing that the controller must carry out when the processing can result in a high risk to the rights and freedoms of individuals (Art. 35 GDPR). The GDPR does not explicitly define what is a high risk, but it exemplifies a few cases where a DPIA will be needed.[85] This is, in particular, the situation where the controller performs a "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Art. 35(3)(a) GDPR). Hence, many AI systems are likely to require a DPIA and the assessment will have to address the risks of discrimination posed by the technology.[86]

---

83 Zuiderveen Borgesius, *op. cit.*, note 1.; Wachter, *op. cit.*, note 54.

84 Zuiderveen Borgesius, *op. cit.*, note 1.

85 Although the Article 29 Working Party (now, European Data Protection Board) has provided some guidelines. See, WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, adopted on 4 April 2017 as last revised and adopted on 4 October 2017, WP 248 rev.01.

86 Zuiderveen Borgesius, *op. cit.*, note 1, p. 22.

Another potential tool to counter algorithmic discrimination is offered by the specific rules in case a fully automatised decision produces legal effects concerning the data subject or similarly significantly affects them (Art. 22 GDPR).[87] In principle, such decisions are forbidden, unless there is an exception, such as the explicit consent of the data subject.[88] And in this latter case, appropriate safeguards should be guaranteed to the individual, so that the latter can challenge the outcome of the decision.[89]

However, also the GDPR presents some loopholes when applied to the problem at stake.

The preliminary limitation is that data protection applies only if the processing concerns personal data, and not all algorithmic operations necessary process personal data.[90] For example, the GDPR might not apply to predictive models: they might be elaborated through the analysis of personal data (to find for example correlations between food preferences and creditworthiness), but the model as such uses mere statistical inferences.

The effectiveness of the principle of transparency and corresponding measures has also been questioned. The existence and the actual boundaries of the "right to explanation" have been at the centre of a lively debate and many scholars are sceptical about its effectiveness.[91] The prohibition under Art. 22 applies only to fully automated decisions, it is not always easy to define in a clear way if the decision can significantly negatively affect individuals, and, in any case, it is not an absolute prohibition.[92] It can be authorized in three important circumstances: a) the explicit consent of the individual; b) legislative provision; c) contractual necessity.[93]

Even when the right to information about the logic behind the algorithm is triggered, a series of obstacles (technical and legal) remain. As previously mentioned, algorithms can be so complex that their logic remains difficult to comprehend even for their developers. If the logic is intelligible, it might be challenging to

87 *Ibid.*; Wachter; Mittelstadt, *op. cit.*, note 60; Wachter, *op. cit.*, note 54.

88 See, Art. 22(2) GDPR.

89 Art. 22(3) GDPR.

90 Zuiderveen Borgesius, *op. cit.*, note 1, pp. 24-25.

91 Wachter; Mittelstadt; Floridi, *op. cit.*, note 82; Edwards; Veale, *op. cit.*, note 82.

92 It has to be noticed, however, that the formulation of such a right in the Modernised Convention 108 is broader as it does not refer to solely automated decisions nor to "the significant effects" for individuals. See, Zuiderveen Borgesius, *op. cit.*, note 1, p. 24.

93 Art. 22(2) GDPR.

translate that information in a meaningful way for laypeople.[94] Moreover, the explanation might be hampered in practice by trade secret protection.[95]

Another set of limitations concerns the rules on sensitive data. Their processing is subject to a higher standard of protection. However, the list of protected grounds is quite narrow and it does not include other vulnerable categories or sensitive information such as sex or socio-economic information.[96]

Moreover, the list contained in Art. 9 GDPR is a *numerus clausus*. Hence, it might be difficult to apply the GDPR protection on sensitive data to, for example, inferred data (non-sensitive as such) leading to a discriminatory outcome.[97]

However, it must be said that the list of special categories of data offers some possibilities for an extensive interpretation (Art. 9 GDPR includes expressions like "data revealing racial or ethnic origin" or "data concerning health"). This wording suggests that sensitive characteristics can be inferred directly but also indirectly.[98] For instance, as recently stated by the CJEU, the publication of information about a spouse's details can indirectly reveal the sexual orientation of the data subject. [99] Hence, it should be considered sensitive data. However, the decision refers to an inference made "following an intellectual operation involving deduction or cross-referencing."[100] It remains to be seen to what extent this reasoning could cover more complex elaborations that could nevertheless cause discrimination.

Finally, even if Data Protection Authorities can play an important role in ensuring the application of the GDPR, there is the concrete problem that many of them are usually understaffed or under-resourced, and they might not be supported by technical experts (which are crucial in a field like algorithmic discrimination).[101] Therefore, the enforcement powers recognized by the GDPR might be more difficult to be exercised in practice.

Also in the field of data protection, several proposals have been presented to improve the existing framework.

---

94 Edwards; Veale, *op. cit.*, note 82.

95 Malgieri, *op. cit.*, note 60; Wachter; Mittelstadt, *op. cit.*, note 60.

96 Zuiderveen Borgesius, *op. cit.*, note 1; Wachter, *op. cit.*, note 54.

97 Wachter, *op. cit.*, note 54.

98 See, Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601, Opinion of AG Pikamäe, para 85.

99 Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601.

100 *Ibid.*, para. 123.

101 Zuiderveen Borgesius, *op. cit.*, note 1.

As previously mentioned, one of the main shortcomings of data protection in the field of algorithmic discrimination is that not all harmful inferences might be classified as personal data or benefit from the stronger protection reserved for sensitive data.

To enhance this level of protection, Wachter and Mittlestadt have proposed the introduction of a new right: the right to reasonable inferences.[102] This right would address the harmful consequences of high-risk inferences. According to the authors, these latter should include inferences that: a) violate privacy or have the potential to harm someone's reputation now or in the future, or b) are based on opinions or have little possibility of verification but are still used to make crucial decisions.[103]

In order to be effective, this right would be formed of an *ex ante* justification mechanisms and an *ex post* control.[104]

The *ex ante* justification would require controllers to explain and justify "(1) why certain data are a normatively acceptable basis to draw inferences; (2) why these inferences are normatively acceptable and relevant for the chosen processing purpose or type of automated decision; and (3) whether the data and methods used to draw the inferences are accurate and statistically reliable."[105]

In addition to that, the individual would have the *ex post* right to contest the unreasonable inference and provide additional information that could lead to an alternative outcome.[106] According to the authors, this right would complement the right to contest the decision at Art. 22 GDPR.

The same authors articulate a more comprehensive set of recommendations to address high risks inferences.

First, they notice that the current scope of data protection – in order to adequately protect individuals - should be expanded to include "the assessment of the reasonableness of inferential analytics and accuracy of decision-making processes."[107]

Second, they recognise that the level of protection depending on the categorisation of personal, non-personal, and sensitive data, is not effective anymore in the

---

102 Wachter; Mittelstadt, *op. cit.*, note 60.

103 *Ibid.*, p. 580.

104 *Ibid.*

105 *Ibid.*, p. 581.

106 *Ibid.*, p. 588.

107 *Ibid.,* p. 614.

Big Data environment. Neutral data can cause the same harm as sensitive data. A predictive model based on anonymous data can be as privacy-invasive as those created from personal data. Hence, they argue that future legislative interventions or judicial interpretations should focus more on how data is used and its impact and rely less on the concept of identifiability.[108] Thus, they should recognise appropriate redress mechanisms when a predictive model is applied to individuals.

Third, to appropriately support the mechanisms of the right to reasonable inferences, future policy interventions should provide for an obligation of the controller to justify the data sources and the intended inferences, and an ability for the data subject to contest the decision. [109]

Among the other data protection tools that could be used to combat algorithmic discrimination, DPIAs figure prominently. However, in practice, DPIAs focus mainly on data security and data quality (and not other substantial aspects that could help address deeper societal issues).[110] Multi-layered models of Algorithmic Impact Assessment (AIA) have been then proposed to complement the existing system.

Mantelero, for instance, introduced the idea of the Human Rights, Social and Ethical Impact Assessment (HRESIA), a more comprehensive tool for AI developers and providers for assessing the impact of their IT solutions.[111] This tool relies on two main components: on the one hand, self-assessments, questionnaires, and risk assessment instruments; and, on the other hand, consultation with experts. According to Mantelero, the universalist dimension of the HRESIA can provide a framework for "the collective dimension of data use"[112], providing a further tool for protecting non-traditional groups created by algorithms.

Kaminski and Malgieri recognise as well that DPIAs do not work perfectly as AIA.[113] However, the GDPR's DPIA is a useful starting point for designing a solid AIA. They suggest the key elements that this model should have. For example, it should involve civil society as an additional form of oversight, the assessment should consider not only the technology in isolation but in its context of use and

---

108 *Ibid.,* pp. 615-618.

109 *Ibid.,* p. 619.

110 As noticed by Kaminski, M. E.; Malgieri, G., *Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR*, in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020.

111 Mantelero, A., *AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment*, Computer Law & Security Review, Vol. 34, No. 4, 2018, p. 754.

112 *Ibid.*, p. 771.

113 Kaminski; Malgieri, *op. cit.*, note 110.

on a system-wide level to mitigate social harms, and most importantly, the system should guarantee individual, group and systemic explanations (what they call "multi-layered explanations").[114]

On a more general level, scholars have shown how the problem of the new forms of differentiations that are created by machine learning is calling for a revision of the current legal frameworks and the adoption of new forms of protection. These new interventions should be grounded on empirical evidence and research.[115]

For instance, Borgesius has pinpointed several measures that could improve the *status quo*, such as the provision of more support to Equalities Bodies and Data Protection Authorities and closer collaboration between them (given the mutual interaction between anti-discrimination and data protection law)[116], and the possibility of carving out a broader research exception to intellectual property protecting the algorithm.[117] To complement these measures, education and research remain crucial: special campaigns aimed at the general public could be launched, and Fairness, Accountability, and Transparency (FAccT) studies should be further supported.[118]

6. CONCLUSIONS

Nowadays, AI-powered decision-making systems are routinely used in many sectors and activities. However, their introduction should be carefully assessed and evaluated. As a growing study of literature demonstrates, fully or partly automated can replicate existing biases or create new and more subtle forms of discrimination.

This paper offered an overview of these risks and the ethical and legal attempts to address them.

To develop trustworthy AI, ethical guidelines can serve as a basis. However, big tech companies need to refrain from the instrumentalisation of ethical language for the purpose of profit and self-regulation. It is important to properly apply moral philosophy in development for the benefit of society at large.

From a legal point of view, the anti-discrimination and data protection frameworks provide an array of tools and remedies to combat algorithmic discrimination. This

---

114 *Ibid.*

115 Zuiderveen Borgesius, *op. cit.*, note 1.

116 *Ibid.*, p. 35.

117 *Ibid.*, p. 65.

118 *Ibid.*, p. 28.

framework, however, does not adequately cover the new situation of harm generated by algorithms. To this end, many authors have argued for introducing specific rules or functional interpretations of the current law to close the loopholes.

In this paper, we have provided a blueprint for analysing a complex and dynamic field. Technology is advancing rapidly, but keeping these tools under vigilant and critical scrutiny is crucial in a democratic society. Our legal framework should respond to these challenges in a timely and meaningful way. Hence, a broader consideration of the issues raised by algorithmic discrimination should find a place in the initiatives tabled by the European legislator, such as the proposed Artificial Intelligent Act, which is currently under discussion.

REFERENCES

BOOKS AND ARTICLES

1. Adams-Prassl, J.; Binns, R.; Kelly-Lyth, A., *Directly Discriminatory Algorithms*, The Modern Law Review, Vol. 86, No. 1, 2023, pp. 144-175
2. Barocas, S.; and Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, Vol. 104, No. 3, 2016, pp. 671-732
3. Broussard, M., *Artificial Unintelligence: How Computers Misunderstand the World*, First MIT Press paperback edition, The MIT Press, 2019
4. Buolamwini, J.; Gebru, T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in: Proceedings of Machine Learning Research, No. 81, Conference on fairness, accountability and transparency (PMLR 2018), 2018, pp. 1-15
5. Cowgill, B. et al, *Biased Programmers? Or Biased Data? A Field Experiment in Operationalizing AI Ethics*, in: Proceedings of the 21st ACM Conference on Economics and Computation, 2020, pp. 1-5
6. Edwards, L.; Veale, M., *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, Duke L. & Tech. Rev., Vol. 16, No. 1, 2017, pp. 18-84
7. Elettra, B., *From Ethics Washing to Ethics Bashing: A View on Tech Ethics from Within Moral Philosophy*, 2021, pp. 1-15, Available at SSRN: [https://ssrn.com/abstract=3914119].
8. Goodman, B.; Flaxman, S., *EU Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, AI Magazine, Vol. 38, No. 3, 2017, pp. 50-57
9. Kaminski, M. E., *The Right to Explanation, Explained*, in: Sandeen, S. K.; Rademacher, C.; Ohly, A. (eds.), Research Handbook on Information Law and Governance, Edward Elgar Publishing, Cheltenham, 2021, pp. 278-299
10. Kaminski, M. E.; Malgieri, G., *Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR*, in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020, pp. 68-79
11. Kearns, M.; Aaron Roth, A., *The Ethical Algorithm: The Science of Socially Aware Algorithm Design*, Oxford University Press, Oxford, 2020

12. Malgieri, G., *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*, International Data Privacy Law, Vol. 6, No. 2, 2016, pp. 102-116
13. Malgieri, G.; Comandé, G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law, Vol. 7, No. 4, 2017, pp. 243-265
14. Mantelero, A., *AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment,* Computer Law & Security Review, Vol. 34, No. 4, 2018, pp. 754-772
15. O'Neil, C., *Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, 2018
16. Selbst, A.; Powles, J., *Meaningful Information" and the Right to Explanation*, in: Proceedings of the 1st Conference on Fairness, Accountability and Transparency (PMLR 2018), Vol. 81, 2018, p.1
17. Selmi, M., *Algorithms, Discrimination and the Law*, Ohio State Law Journal, Vol. 82, No. 4, 2021, pp. 611-651
18. European Union Agency for Fundamental Rights, *Handbook on European Non-Discrimination Law*, Publications Office of the EU, Luxembourg, 2018
19. Wachter, S., *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, Berkeley Tech. LJ, Vol. 35, No. 2, 2020, pp. 367-430
20. Wachter, S., *The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Anti-Discrimination Law*, Tulane Law Review, Vol. 97, No. 2, 2022, pp. 1-50
21. Wachter, S.; Mittelstadt, B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. L. Rev., No. 2, 2019, pp. 494-620
22. Wachter, S.; Mittelstadt, B.; Floridi, L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, Vol. 7, No. 2, 2017, pp. 76-99
23. Webb, A., *The Big Nine*, Ingram Publisher Services US, 2019
24. Xenidis, R., *Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience*, Maastricht Journal of European and Comparative Law, Vol. 27, No. 6, 2021, pp. 736-758
25. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, First Trade Paperback Edition, Public Affairs, 2020

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-152/11 *Johann Odar v Baxter Deutschland GmbH* [2012] ECLI:EU:C:2012:772
2. Case C-528/13 *Geoffrey Léger v Ministre des Affaires sociales, de la Santé et des Droits des femmes and Etablissement français du sang* [2014] ECLI:EU:C:2014:2112, Opinion of AG Mengozzi
3. Case C-443/15 *David L. Parris v Trinity College Dublin and Others* [2016] ECLI:EU:C:2016:493, Opinion of AG Kokott
4. Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601

5. Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601, Opinion of AG Pikamäe

COUNCIL OF EUROPE

1. Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108, as amended by Protocol, 18 May 2018, CETS 223
2. European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5

EU LAW

1. Charter of Fundamental Rights of the European Union [2012] OJ C 326
2. Council Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/2000
3. Council Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation [2000] OJ L303/2000
4. Council Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L373/2004
5. Directive 2006/54/EC of the European Parliament and of the Council on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L204/2006
6. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017 as last revised and adopted on 4 October 2017, WP 248 rev.01.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L119/2016
8. Treaty on European Union (Consolidated version) [2016] OJ C 202
9. Treaty on the Functioning of the European Union (Consolidated version) [2016] OJ C 202

REPORTS

1. Fredman, S., *Intersectional Discrimination in EU Gender Equality and Non-Discrimination Law*, European Commission, Brussels, 2016
2. High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, Brussels, 2019
3. Zuiderveen Borgesius, F., *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*, Council of Europe, Strasbourg, 2018

UDK 342.7:341.9]:004
Original scientific paper

PRIVATE INTERNATIONAL LAW AS A MEANS TO PROJECT EU DIGITAL VALUES ABROAD*

Edoardo Benvenuti, PhD, Postdoctoral Fellow
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
edoardo.benvenuti@unimi.it

ABSTRACT

In light of the pivotal role that new technologies play for the achievement of policy objectives, and considering their ability to negatively affect rights and freedoms in a ubiquitous manner, EU law is adopting a number of instruments to regulate those matters that are particularly influenced by digitalisation. Such instruments include substantive rules applicable to several online activities. This legislation aims at establishing an environment where digital interactions take place in accordance with fundamental rights, whose protection is enshrined within EU primary law, as well as to ensure the proper functioning of the internal market. Given the ubiquitous nature of digital technologies, and in order for these rules to be effective, their scope of application is designed to also include cases that may be strongly related to Third States. In this way, the EU aims at strengthening its digital sovereignty by creating a strong digital single market, and by guaranteeing the protection of European users, whose rights should benefit from the protection of EU substantive law even when digital activities take place abroad.

Although the EU has a strong interest in ensuring a broad application of its substantive rules, the possibility for EU law to be concretely applicable abroad depends – in the first place – on the existence of jurisdictional rules specifically designed to apply to disputes that may involve parties from Third States. Nonetheless, while some of the instruments adopted in this area ensure the application of substantive rules by providing for specific grounds of jurisdiction, litigation in these matters will normally fall within the scope of Regulation (EU) n. 1215/2012, whose rules apply – in general – only when the defendant has her/his domicile in the Union.

In light of these considerations, the paper will assess the coherence between the broad scope of some of the instruments that the EU has adopted (or is going to adopt) in fields strongly affected by digitalisation – such as the GDPR, as well as other EU's initiatives pertaining to Artificial

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Intelligence and to digital platforms – and Regulation (EU) n. 1215/2012, in order to evaluate the ability of the latter to support the application of EU digital standards world-wide.

***Keywords**: Digitalisation, online infringement, personality rights, private international law, jurisdiction, Third States*

1. INTRODUCTION

In a number of fields, the European Union (EU) is promoting the dissemination of its policies world-wide.[1] Such phenomenon has been analysed by scholars, who distinguished (at least) two main "techniques", through which the EU is – *de facto* – exercising its regulatory power globally.[2]

On the one hand, the European legislature is adopting substantive rules that are designed to apply when a territorial link with the EU is established, for example, by virtue of activities that, although carried out in a Third State, produce their effects within the Union.[3] On the other hand, the EU does not impose the unilateral application of its rules, but it rather creates incentives that encourage foreign companies to voluntarily adhere to its standards in order for them to operate in the European market.[4]

EU's inclination to act as a "global regulator" is justified by multiple reasons, one of the main causes of the spread of EU values abroad being related to digitalisation. As a matter of fact, digital technologies contribute to create an environment where interactions are dematerialised, and where the principle of territoriality cannot be applied according to its traditional meaning.[5] Moreover, in light of their ubiquitous nature, digital activities and operations that avail themselves of sophisticated technologies are particularly insidious, as they can easily impair fundamental rights, whose protection is enshrined within EU primary law.[6] These circumstances make the need to control and regulate foreign activities even more urgent.

Due to its peculiar features, digitalisation affects the concept of jurisdiction on at least two levels.

---

1 On this topic, see Cremona, M.; Scott, J. (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, 2019.

2 See Scott, J., *Extraterritoriality and Territorial Extension in EU Law*, The American Journal of Comparative Law, Vol. 62, No. 1, 2014, pp. 87–125; Bradford, A., *The Brussels Effect: How the European Union Rules the World*, New York, 2020.

3 This is the so called "territorial extension" of EU law, on which see Scott, *op. cit.*, note 2.

4 See Bradford, *op. cit.*, note 2.

5 See Chia, C. W., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, Singapore Academy of Law Journal, Vol. 30, No. 2, 2018, pp. 833–870.

6 Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (CFREU).

In the first place, the non-territorial nature of the Internet imposes adjustments in the application of rules regulating activities that take place online. The scope of the instruments adopted by the EU in this field must necessarily include activities that, while not taking place in the Member States, are likely to compromise EU's interests. Accordingly, EU law in this field is designed to apply not only to persons and undertakings operating from the Union, but also to those that, albeit located in Third States, direct their activities to Member States through the Internet or by means of digital technologies.

Secondly, the non-territorial nature of the Internet affects the issue of jurisdiction from the perspective of private international law (PIL). Indeed, the concrete application of EU standards to companies and persons located abroad depends on the possibility to enforce the rights enshrined in EU law (even) when one of the parties to a dispute is domiciled in a non-EU State. Thus, rules on jurisdiction have paramount importance: the law applicable to transnational litigations is determined through the conflict-of-laws rules of the forum; consequently, the existence of rules on jurisdiction specifically designed to attract this kind of disputes before a court in a Member State has a key-role in ensuring the application of EU rules when activities taking place abroad are involved. From this point of view, PIL is an important tool for the regulation of matters strongly affected by digitalisation, as it contributes to the projection of EU digital values abroad.[7]

In light of these considerations, the present paper aims at assessing the role of EU PIL in regulating online activities and in projecting EU policies and values pertaining to digital matters abroad. For this purpose, I will take into account some of the main instruments that the EU has adopted (or that it is going to adopt) in digital matters. Since the scope of such instruments normally transcends Member States' borders, I will evaluate the ability of EU rules on adjudicative jurisdiction to support the "extraterritorial" application of EU substantive rules in this field.

2. THE "EXTRATERRITORIAL" SCOPE OF EU POLICIES IN DIGITAL MATTERS

Due to the paramount relevance of the interests that are normally at stake in matters affected by digitalisation, the main concern of each legal system is to ensure

[7] In relation to the potential role of PIL in contributing to the regulation of matters related to the Internet, see Lutzi, T., *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 129–145; Pretelli, I., *Protecting Digital Platform Users by Means of Private International Law*, Cuadernos de Derecho Transnacional, Vol. 13, No. 1, 2021, pp. 574–585.

the application of its own standards with respect to activities that might undermine those values. In fact, in regulating this field, States may give relevance to different policies; as a consequence, the conclusion of international agreements pertaining to this area of law appears to be a difficult outcome to achieve, since each Country will try to prioritise its own policies during the drafting process. Under this perspective, the unilateral adoption of substantive rules with a broad territorial scope thus remains the preferable solution, especially when digital activities risk impairing fundamental rights.

The need to ensure the protection of fundamental rights with respect to activities incorporating high-tech features is especially evident when it comes to data protection law: while the European approach pays special attention to the protection of personal data,[8] other legal systems give priority to different policies or do not ensure natural persons a level of protection that is sufficiently high according to EU standards.[9]

However, data protection law is not the only example of how the EU displays the ambition to spread its digital values in Third States, as the European legislature adopted (and is going to adopt) a number of acts that are meant to apply not only within the Union, but also abroad. In fact, the scope of application of this legislation goes beyond the borders of the Member States, and it is usually defined according to criteria that, although territorial in nature, end up triggering a sort of extraterritorial effect. These rules may then be relevant not only in perfectly intra-EU cases, but also when the proceedings are brought against subjects that are not based nor operate within the Union.

---

8 At the Council of Europe level, the protection of personal data has been essentially pursued through Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11, 14 and 15, 4 November 1950, ETS 5 (ECHR), as well as through the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108; with respect to the application of Art. 8 ECHR in the field of data protection, see, *inter alia*, judgment *Amann v Switzerland* (2000) 30 EHRR 843. At the EU level, the need to ensure the protection of personal data not only stems from EU secondary law instruments, but it is also enshrined in Art. 8 CFREU. Moreover, Art. 16 TFEU (Treaty on the Functioning of the European Union [2007] OJ C 326/01) empowers the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data. On the protection of personal data according to the European approach, see Vogiatzoglou, P.; Valcke, P., *Two decades of Article 8 CFR: A critical exploration of the fundamental right to data protection in EU law*, in: Kosta, E.; Kamara, I.; Leenes, R. (eds.), Research Handbook on EU Data Protection Law, Northampton, 2022, pp. 11–49.

9 See, in particular, the judgment of the Court of Justice of the EU (CJEU) in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] not yet published.

2.1. The scope of EU data protection law

Within the framework of EU law, the matter at stake is currently regulated by the General Data Protection Regulation (GDPR),[10] which repealed the Data Protection Directive.[11] In line with the abrogated instrument, the GDPR aims at removing the obstacles to flows of personal data within the EU by creating a level of protection of the rights and freedoms of natural persons with regard to the processing of their personal data that is equivalent in all Member States.[12] The protection of natural persons in relation to the processing of their personal data is thus a policy objective that is not only relevant not only for its implication on human rights, as it is also instrumental in guaranteeing the proper functioning of the internal market. Under this perspective, the adoption of a Regulation in this field – which is, in principle, directly binding in all its parts[13] – is aimed at ensuring a greater level of harmonisation within the EU, since the margin of appreciation left to the Member States in the implementation of the Data Protection Directive was addressed as one of the main shortcomings of the previous regime in reaching the aforementioned goals.[14]

In order to achieve such goals, EU legislation in this field is conceived not only to apply to data processing that is entirely conducted in a Member State. Under this perspective, the Regulation reproduces the tripartite division adopted by the Directive, even though the GDPR's scope of application is shaped according to elements that partially diverge from those employed in the context of the Data Protection Directive,[15] as the Regulation was specifically designed to have a wide

---

10 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [2016] OJ L 119/1 (General Data Protection Regulation).

11 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive).

12 In particular, see Recital 10 of the GDPR.

13 Nonetheless, it has been pointed out that the GDPR still leaves room for manoeuvre for Member States, since several aspects of its implementation require the intervention of national legislators in order to regulate specific issues of the data protection regime. This situation, together with the lack of an explicit conflict-of-laws rule, open up to possible private international law challenges. On this topic, see Mantovani, M., *Horizontal Conflicts of Member States' GDPR-Complementing Laws: The Quest for a Viable Conflict-of-Laws Solution*, Rivista di diritto internazionale privato e processuale, Vol. 55, No. 3, 2019, pp. 535–562.

14 See Hustinx, P., *EU Data Protection Law: The Review of Directive 95/46/CE and the General Data Protection Regulation*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford, 2017, pp. 148–151.

15 De Miguel Asensio, P., *Conflict of Laws and the Internet*, Cheltenham and Northampton, 2020, pp. 134–135.

international dimension.[16] As a result, it was suggested that the adoption of the GDPR would have been an opportunity to expand the scope of application of EU data protection law, as to ensure the coherent application of EU standards against both EU based and non-EU based undertakings, thus leading to benefits in terms of fair competition.[17]

First, according to Art. 3(1) of the GDPR, non-EU undertakings can be subject to the application of the Regulation when they are considered to have an establishment in one or more Member States.[18] Such evaluation should be carried out *in concreto*, and in light of the rather broad terms defined by the CJEU with regard to the criteria set forth in the Directive. Notably, in *Google Spain*, the CJEU gave an extensive interpretation of Art. 4(1)(a), according to which national provisions adopted pursuant to the Data Protection Directive applied to the processing of personal data "where the processing (was) carried out in the context of the activities of an establishment of the controller on the territory of (a) Member State".[19] In this regard, the CJEU focused on the meaning of the expression "an establishment", and adopted a teleological interpretation of the criterion in order to ensure the achievement of the human rights goals set forth in the Data Protection Directive.[20] Accordingly, the CJEU stated that the processing of personal data for the purposes of the service of a search engine having its seat in a Third State and an establishment in a Member State was carried out "in the context of the activities" of that establishment, even when the latter was not directly involved in the processing activities but it only carried out marketing activities in order to make

16 Hustinx, P., *op.cit.*, note 14, p. 155.

17 Redic, V., *The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights*, 2014, [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_175], Accessed 24 July 2023. See also European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 4.

18 See Art. 3(1) of the GDPR, which states that the Regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". Interestingly, Art. 4 of the GDPR (headed "Definitions") does not provide a definition of "establishment" for the purpose of Art. 3(1), as Art.4(16) only defines the notion of "main establishment", which is mainly relevant in order to determine the competence of the lead supervisory authority according to Art. 56 of the GDPR. Nonetheless, some clarifications with regard to the definition of "establishment" are provide by Recital22 of the GDPR, which substantially reproduces the wording of the abovementioned CJEU's case-law.

19 It is worth noting that, in addition to the "establishment" criterion, Art. 3(3) of the GDPR confirms the application of EU data protection law also when the processing takes place where Member State law applies by virtue of public international law, which was first incorporated in Art. 4(1)(b).

20 de Hert, P.; Czerniawski, M., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Vol. 6, No. 3, 2016,, pp. 234–235.

the service offered by that engine profitable.[21] In the CJEU's view, such conclusion was justified in light of the paramount importance of the right to privacy, which imposed to not interpret the wordings of Art. 4(1)(a) restrictively.[22]

Moreover, if it is not possible to include a non-EU controller or processor within the scope of EU data protection law through Art. 3(1) of the GDPR, it is possible to refer to other criteria set forth in the Regulation.[23] In particular, while Art. 4(1)(c) of the Data Protection Directive adopted the location of the equipment as a criterion to determine the application of EU law against controllers not established in the Union,[24] the GDPR's approach is shaped on the basis of a targeting test. In fact, Art. 3(2) states that the Regulation also applies "to the processing of

---

21 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzále* [2014] published in the electronic Reports of Cases, par. 55. See also Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] published in the electronic Reports of Cases, paras. 19–41, in which the Court stated that a controller that exercises, through stable arrangements in a Member State, a real and effective activity in the context of which the processing is carried out, will be considered to have an "establishment" in that Member State, even when such activity appears to be "minimal" in the context of the processing of data. Such interpretation applies even when the controller is registered in a different Member State or in a Third State.

22 Case C-131/12 *Google Spain and Google*, note 21, par. 53. In several occasions the CJEU recalled that the protection of fundamental rights represented the guiding principle through which it developed its case-law concerning the (broad) scope of the Data Protection Directive (see, *ex multis*, Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] published in the electronic Reports of Cases, par. 26).

23 See European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 9.

24 According to Art. 4(1)(c), national provisions adopted by Member States pursuant to the Directive applied where the controller, albeit not established in the EU, processed personal data making use of equipment, automated or otherwise, situated on the territory of a Member State, unless such equipment was used only for purposes of transit through the territory of the Union. See also Recital 20 of the Directive, according to which "Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice" (emphasis added). Even though some scholars emphasised the terminological shift from the term "means" of the Recital20 to the term "equipment" of Art. 4(1)(c), addressing that it represented the attempt of the EU legislature to narrow the scope of Art. 4(1)(c).(see Moerel, L., *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, International Data Privacy Law, Vol. 1, No. 1, 2011, p. 33), such a reading collided with the case-law of the CJEU on Art. 4, as well as with the interpretation suggested by the Article 29 Data Protection Working Party, according to which the term "equipment" should have been understood in broad terms (Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836-02/10/EN, WP 179, p. 19). The meaning of the term "equipment" could have been clarified by the CJEU in *Rease and Wullems*, but the case was dismissed (Case C-192/15, *T. D. Rease and P. Wullems v College bescherming persoonsgegevens* [2015] OJ C78/11). On this topic, see de Hert, P.; Czerniawski, M., *op.cit.*, note 20, p. 236.

personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;[25] or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union".[26] The declared intention of the targeting test incorporated in Art. 3(2) of the GDPR is to ensure the protection of natural persons according to the provisions enshrined therein.[27]

This approach appears to be consistent with the criteria that, according to public international law, justify the extraterritorial intervention of a given legal system, since EU jurisdiction against processing activities by controllers or processors that are not established in a Member State is only triggered where those activities are in some way connected to the EU.[28] Accordingly, the extension of the scope of application of EU data protection law, which represents an important rationale of the reform,[29] has been pursued by requiring some sort of territorial link between the processing activities and the EU.[30] In fact, on the one hand, Art. 3(1) ensures that the territorial application of the GDPR against a non-EU controller/processor is triggered by the presence in the Union of an "establishment" in the context of whose activities the processing is carried out, while the place where the processing is carried out and the geographical location of data subjects are not relevant for the purpose of Art 3(1);[31] on the other, Art. 3(2) employs a targeting test that gives relevance to the presence of data subjects within the EU, in order to ensure the effective protection of fundamental rights.

---

25 Art. 3(2)(a) of the GDPR.

26 Art. 3(2)(b) of the GDPR.

27 Recital 23 of the GDPR.

28 De Miguel Asensio, P., *op. cit.*, note 15, p. 135. The importance of public international law restrictions in this field has also been underlined by the Commission in its amicus brief released in relation to the *Microsoft Warrant* case (European Commission amicus brief, *United States v Microsoft Corporation* [2017] No. 17-2, pp. 5–8). On this point, see Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 76–77.

29 See note 17.

30 Svantesson, D. J. B., *op. cit.*, note 28, p. 76.

31 See European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020), p. 14, that underlines that this approach is supported by Recital 14 of the GDPR, which states that "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data".

2.2. The scope of EU's approach to Artificial Intelligence

The EU Commission is currently working on the adoption of several instruments in the field of Artificial Intelligence (AI), which are meant to benefits the internal market by regulating a framework on the usage of AI-systems, in order to foster the free movement of AI-based goods and services cross-border while ensuring a high level of protection of health, safety and fundamental rights. In light of both the policy objectives underlying this legislation and the possible cross-border impacts of the employment of AI-systems, the proposed instruments are likely to apply in situations involving actors established outside the EU.

More specifically, the proposed Artificial Intelligence Act (AI Act Proposal)[32] – which aims at imposing obligations for several actors in the value chain – strives to have a manifestly broad scope, since it proposes to apply to providers placing on the market or putting into service AI-systems in the Union, irrespective of whether those providers are physically present or established within the Union (Art. 2(1)(a)), as well as to users located in the EU (Art. 2(1)(b)).[33] Moreover, according to Art. 2(1)(c), the proposed legislation "should also apply to providers and users of AI-systems that are established in a third country, to the extent the output produced by those systems is used in the Union".[34]

However, as regards the AI Act Proposal, it has been pointed out that some aspects of its scope are vague; in particular, with regard to Art. 2(1)(b), it is not clear whether a temporary presence of the user on the territory of a Member State is sufficient to trigger the application of EU law.[35] Such uncertainties are not completely clarified by the amendments proposed by the EU Parliament,[36] which include new rules pertaining to the scope of application of the AI Act Proposal that – to some extent – appear as vague as those enshrined in the Commission's proposal.

---

32 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 (AI Act Proposal).

33 See Recital 10 of the AI Act Proposal, underlining that the Regulation should apply in a non-discriminatory manner to providers of AI-systems, irrespective of whether they are established within the Union or in a third country, and to users of AI-systems established within the Union.

34 See Recital 11.

35 See Pato, A., *The EU's Upcoming Framework on Artificial Intelligence and its Impact on PIL*, 12 July 2021 [https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/], Accessed 24 July 2023.

36 Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD).

In particular, on the one hand, the amendments aim at changing the aforementioned Art. 2(1)(b) of the AI Act by referring to "deployers" (and not "users") of AI systems that have their place of establishment or who are located within the EU; on the other, (new) Art. 2(1)(cc) states that the Regulation will apply to "affected persons" – as defined in Art. 3(8a)[37] – "that are located in the Union and whose health, safety or fundamental rights are adversely impacted by the use of an AI system that is placed on the market or put into service within the Union".[38] Once again, the latter amendment not only omits to clarify whether a temporary presence on the EU territory is sufficient to trigger the application of the AI Act, but it also refers to concepts – like the one to the "adverse impact" – that are not clearly defined and whose contours are blurred.

Since the AI Act Proposal concerns the public interest, the infringements of its rules may raise issues that appear to pertain mostly to administrative law.[39] Thus, the lack of provisions in the area of private international law is not a surprise. Nonetheless, the proposed instrument plays a pivotal role in the identification of EU policies and definitions in this field; moreover, the instrument's broad scope of application shows that – in order for these policies to be concretely implemented – compliance with EU standards should be ensured at a global level.

Accordingly, the Union is working on the implementation of these policies also from the angle of civil liability. In particular, in 2022, the EU Commission proposed to adopt the Artificial Intelligence Liability Directive (AI Liability Directive Proposal)[40] and to revise the Product Liability Directive,[41] as to make the latter instrument resilient to technological progress.[42] The two instruments follow the

---

37 According to the proposed Art. 3(8a), "'affected person' means any natural person or group of persons who are subject to or otherwise affected by an AI system".

38 In particular, according to the amendments of the EU Parliament, the AI Act should apply to "providers placing on the market or putting into service AI systems referred to in Article 5 outside the Union where the provider or distributor of such systems is located within the Union" (Art. 2(1)(ca)), as well as to "importers and distributors of AI systems as well as authorised representatives of providers of AI systems, where such importers, distributors or authorised representatives have their establishment or are located in the Union" (Art. 2(1)(cb)).

39 With regard to private international law issues within the framework of the AI Act Proposal, see Pato, A., *op. cit.*, note 35.

40 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (AI Liability Directive Proposal).

41 Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29 (Product Liability Directive)

42 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.

EU Parliament's Resolution of 20 October 2020 with recommendations on the adoption of a Regulation on Liability for the Operation of Artificial Intelligence-Systems,[43] which intended to provide a liability regime for AI-related harms by distinguishing between "high-risk AI-systems" (subject to a strict liability mechanism), and "other AI-systems" (subject to a fault-based liability regime).[44] The proposed Directives aim at ensuring the adoption of harmonised rules in the field of civil liability for damages caused by the usage of AI-systems in order to complement the obligations set forth in the AI Regulation Proposal.[45] More specifically, they aim at ensuring the proper functioning of the internal market by: (i) guaranteeing the injured persons the respect of their right to compensation; (ii) increasing the legal certainty about the liability risks that businesses face when doing business; (iii) promoting consumer trust in AI-enabled products and services.

In particular, and in order to ensure the achievement of the aforementioned goals, the AI Liability Directive Proposal intends to increase the changes of successfully obtain redress by providing a system of rebuttable presumptions (Art. 4) and mechanisms on disclosure of evidence aimed at favouring the victims of AI-related harms (Art. 3). For its part, the proposed amendments to the Product Liability Directive clarifies that goods incorporating an AI-system are "products", and that compensation is available when defective AI causes damage, without the injured person having to prove the manufacturer's fault, just like for any other product.

Like the GDPR and the Online Platform Regulation, the proposed legislation aims at applying against non-EU subjects; accordingly, the scope of EU's approach to AI is defined in a broad (and sometimes unclear) manner.

In particular, the territorial scope of the Regulation proposal attached to the EU Parliament's Resolution was defined in light of criteria that appear to be vague; namely, according to Art. 2(1), the application of the proposed instrument is triggered when AI-systems "caused significant immaterial harm resulting in a verifiable economic loss" in the EU, Without further specifying these notions.[46] Thus, the instrument attached to the Parliament's resolution actually defined its scope of

---

43 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) (AI Liability Regime Resolution).

44 See Chamberlain, J., *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, European Journal of Risk Regulation, Vol. 14, No. 1, 2023, pp. 9–12.

45 See Recital 2 of the AI Liability Directive Proposal.

46 On this point, see Poesen, M., *Regulating Artificial Intelligence (AI) in the European Union (EU): Exploring the Role of Private International Law*, X, Recht in beweging – 29ste VRG-Alumnidag 2022, 2022, par. II.2 [Available at SSRN: https://ssrn.com/abstract=3959643 or http://dx.doi.org/10.2139/ssrn.3959643].

application by referring to the criterion of damage, albeit in vague and imprecise terms; this solution would have allowed for the application of the liability rules even to persons domiciled in a Third State.

Similarly, the AI Liability Directive Proposal, as well as the amendments concerning the Product Liability Directive, aims at applying even when some of the subjects within the supply chain are not established in the EU.

As regards the AI Liability Directive Proposal, Art. 1(2) clarifies that it applies to non-contractual fault-based civil law claims for damages caused by an AI system, i.e. regimes that provide for a statutory responsibility to compensate for damage caused intentionally or by a negligent act or omission. The aforementioned AI Act Proposal will play a pivotal role in the identification of the Directive's scope of application. In fact, in order to ensure the coherent application of the proposed legislation, the scope of the AI Liability Directive Proposal is defined according to the definitions provided in the AI Act Proposal,[47] which includes – to some extent – operators and users established outside the EU.[48]

Yet, the approach followed in the field of product liability is slightly different. As a matter of fact, the amendments concerning the Product Liability Directive identify several economic operators – other than the manufacturer – who can be held liable in the event that the manufacturer is established in a Third State (Art. 7).[49] As a matter of fact, the proposed instrument aims at ensuring that "there is always a business based in the EU that can be held liable for defective products bought directly from manufacturers outside the EU, in light of the increasing trend for consumers to purchase products directly from non-EU countries without there being a manufacturer or importer based in the EU".[50] In this way, the issue of the direct application of EU rules against non-EU subjects is (at least in part) circumvented, as the amendments define a series of economic operators in order to enable victims of damages caused by AI-products to file a claim before the authorities of a Member State. Nonetheless, the proposal confirms the EU's tendency to

47 See Recital 26, Art. 2(3) and Art. 2(4) of the AI Liability Directive Proposal.

48 See note 34.

49 See also Recital 27, stating that "In order to ensure that injured persons have an enforceable claim for compensation where a manufacturer is established outside the Union, it should be possible to hold the importer of the product and the authorised representative of the manufacturer liable".

50 See the explanatory memorandum attached to the Proposal, p. 2.

act as a "global regulator", since it aims at affecting non-EU undertakings too,[51] namely in light of the phenomenon known among scholars as "Brussels effect".[52]

2.3. The scope of EU's initiatives in the field of digital platforms

EU's legal instruments and initiatives in matters affected by digital technologies are numerous, and it is not possible to analysed all of them in this contribution. Nonetheless, it seems appropriate to recall, at least, two initiatives undertaken by the European legislature in the field of digital platform: the Regulation (EU) 2019/1150 (Online Platforms Regulation),[53] which regulates the relationship between platforms that provide online intermediation services and businesses using such platforms to supply products or services to consumers, and the Platform Workers Directive Proposal.[54]

The overall objective of the first instrument is to contribute to the proper functioning of the internal market by laying down rules to ensure that business users are granted appropriate transparency, fairness and effective redress possibilities.[55] In particular, given the increased dependence of undertakings that use intermediation services to reach consumers, the providers of those services might have superior bargaining power, enabling them to behave "in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union".[56]

In order for the instrument to be effective, its scope of application is designed in light of the de-materialised nature of the Internet,[57] as well as of the "intrinsic cross-border potential" of the intermediation services and the transactions that such services aim at facilitating.[58] Accordingly, the Regulation applies to online intermediation services and online search engines "irrespective of the place of es-

---

51 *Ibid.*, p. 6, stating that the Directive "will also encourage all businesses, including non-EU manufacturers, to place only safe products on the EU market in order to avoid incurring liability. This will in turn reinforce product safety".

52 See note 4.

53 Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57 (Online Platforms Regulation).

54 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 (Platform Workers Directive Proposal).

55 Art. 1(1) of the Online Platform Regulation.

56 Recital 2 of the Online Platform Regulation.

57 See Recital 9 of the Online Platform Regulation, which emphasises the global dimension of online intermediation services and online search engines.

58 Recital 6 of the Online Platform Regulation.

tablishment or residence of the providers of those services and irrespective of the law otherwise applicable", as long as two cumulative conditions are met: (i) such platforms provide their services to business users established in the Union; and (ii) those business users offer goods and services to consumer located in the EU.[59] As a consequence, the Regulation applies to the relationship between a non-EU based platform operator and a business established in a Member State, as long as the latter makes usage of the former in order to trade with consumers who are located within the EU.

Like the GDPR, the criteria that define the territorial scope of the Online Platform Regulation are thus based on a targeting test, which responds to the ubiquitous features and means that are employed in this field by requesting a link between the activities that the Regulation intends to regulate and the EU; such link is based on the presence – within the EU's territory – of the businesses using the platforms and of the consumers.

Another example can be in the directive proposal that the EU Commission presented on 9 December 2021 in order to improve the working conditions of platform workers.[60] Such initiative aims at improving the protection of this type of workers "by ensuring correct determination of their employment status, by promoting transparency, fairness and accountability in algorithmic management in platform work and by improving transparency in platform work, including in cross-border situations" (Art. 1(1)).

With regard to the policy objectives underlying the proposed legislation, it can be observed that the Council 's General Approach on the Directive[61] clarified the objective scope of the future instrument, and strengthen the link between the platform workers' rights, data protection and AI.[62]

---

59 Art. 1(2) of the Online Platform Regulation. See also Recital 9, clarifying that this criterion should be interpreted in accordance with the relevant case-law of the CJEU on Art. 17(1)(c) of Brussels I-*bis* Regulation and Art. 6(1)(b) of the Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177/6 (Rome I Regulation).

60 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM (2021) 762 (Platform Workers Directive Proposal).

61 General Approach adopted by the Council on 12 June 2023 on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work (Document ST_10758_2023_INIT).

62 See in particular Recital 29, 32, 37, 47 and Art. 1(1) of the proposal included in the General Approach, stating that "The purposes of this Directive are to improve the working conditions of workers and the protection of persons performing platform work, regarding the processing of their personal data through the use of automated monitoring or decision-making systems".

The final goal of the Platform Worker Directive Proposal is thus to prevent the use of digital technologies from impairing the working condition and the rights of the workers, as well to avoid that – by creating new business models and new forms of employment – platform work results in abuses, for example by enabling the employer to take advantage of the blurred boundaries between employment relationships and self-employed activities.[63]

Consistently with the need to ensure the protection of workers' rights, as well as the proper functioning of the internal market, the Platform Workers Directive aims at applying also to non-EU employers, as long as their activities have an impact on the EU market. Namely, according to Art. 1(3) of the Proposal attached to the Council's General Approach, the Directive is meant to apply "to persons performing platform work in the Union, to digital labour platforms organising platform work performed in the Union, irrespective of the platform's place of establishment and irrespective of the law otherwise applicable" (Art. 1(3))".[64]

The scope of the two initiatives in the field of digital platforms is thus consistent with the approach generally adopted by the European legislature in matters affected by digital technologies, as it is designed to transcend the borders of the EU's territory, in order to ensure the comprehensive and coherent application of EU law, as well as the complete achievement of EU's policy objectives.

3. EU RULES ON INTERNATIONAL JURISDICTION WITHIN THE CONTEXT OF ONLINE ACTIVITIES

As already mentioned, the unilateral adoption of legal instruments with a broad territorial scope is not sufficient to ensure the application of EU law in situations that are strongly connected to Third States. In fact, even though the recalled EU

---

63 See Recital 6 of the proposal included in the General Approach. In this regard, it should also be pointed out that the CJEU clarified that the status of "worker" within the meaning of EU law is an autonomous concept, as "the classification of a 'self-employed person' under national law does not prevent that person being classified as an employee within the meaning of EU law if his independence is merely notional, thereby disguising an employment relationship" (Case C-413/13 *FNV Kunsten Informatie en Media v Staat der Nederlanden* [2014] published in the electronic Reports of Cases, par. 35).

64 See Art. 1(2) of the Commission's Proposal (which the General Approach intends to abrogate), according to which the Directive "lays down minimum rights that apply to every person performing platform work in the Union who has, or who based on an assessment of facts may be deemed to have, an employment contract or employment relationship as defined by the law, collective agreements or practice in force in the Member States with consideration to the case-law of the Court of Justice. In accordance with Article 10, rights laid down in this Directive pertaining to the protection of natural persons in relation to the processing of personal data in the context of algorithmic management also apply to every person performing platform work in the Union who does not have an employment contract or employment relationship".

legislation defines the spatial scope of its rules according to criteria that include non-EU subjects or activities taking place abroad, the interest of the EU to apply its own rules extraterritorially might collide with the parallel interest of other legal systems to regulate the same situations according to policies that are divergent from those of the EU. As a consequence, in order to ensure the coherent application of EU law, it is not enough to expect non-EU undertakings to adhere to EU standards when their activities have a more tenuous connection with the European Union, but it is also fundamental to ensure that EU subjects have the opportunity to concretely enforce their rights against non-EU operators.

3.1. The "general" application of the Brussels I-bis Regulation to relationships presenting digital elements

Since the concrete application of a given legal act in cross-border cases requires the actual opportunity to seek a judicial remedy where the rights conferred under the act itself have been violated, it is apparent the connection between prescriptive and adjudicatory jurisdiction. Accordingly, several EU acts deal with adjudicatory jurisdiction in cross-border cases, and in particular the Brussels I-*bis* Regulation, which – among other things – lays down jurisdiction rules in the field of civil and commercial matters.[65]

The application of the Brussels I-*bis* Regulation is "general", since – in the lack of specific rules on international jurisdiction in other sectorial instruments of the EU – the grounds for jurisdiction enshrined therein apply to any proceedings in the field of civil and commercial law, as long as such proceedings fall outside the excluded matters that are listed in Art. 1 of the Regulation itself.[66] As a matter of fact, the notion of "civil and commercial matters" encompasses a great number of fields, among which data protection and, more generally, contractual and non-contractual relationships presenting a digital element; thus, the Brussels I-*bis* Regulation applies not only to proceedings in the field of data protection law,[67] but virtually to any civil claim originating from a digital infringement.

---

65 Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351/1.

66 Franzina, P., *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in: De Franceschi, A. (ed.), European Contract Law and the Digital Single Market. The Implications of the Digital Revolution, Cambridge, 2017, p. 87.

67 See Requejo Isidro, M., *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection*, MPILux Research Paper Series, No. 3, 2019, [Available at SSRN: https://ssrn.com/abstract=3339180 or http://dx.doi.org/10.2139/ssrn.3339180], section 3.2.1. See also Brkan, M., *Data*

Under the Brussels I-*bis* Regulation, a person (e.g. a data subject) who considers that his or her rights have been infringed by means of an unlawful activity presenting a digital element (e.g. a processing activity) may – in principle – sue the counterparty (e.g. the controller/processor) before the courts of multiple Member States, and in particular: (i) under Art. 4(1), in the place of domicile of the defendant;[68] (ii) under Art. 7(1), where the activity takes place in the context of the performance of a contract, in the place of performance of the obligation in question, as defined by the rule itself; (iii) under Art. 7(2), in matters relating to tort, delict or quasi-delict (including pre-contractual liability),[69] in the place where the harmful event occurred or may occur, with the clarification that such place includes both the place where the damage occurred and the place of the event giving rise to it,[70] notwithstanding the possibility for the victim of a personality right infringement to file a claim in the Member State where he/she has his/her centre of interests;[71] (iv) under Art. 7(5), with regard to a dispute arising out of the operations of a branch, agency or other establishment, in the place where the branch, agency or other establishment is situated; (v) under Art. 25, in the place indicated by the parties in a prorogation agreement (such jurisdiction shall be exclusive unless the parties have agreed otherwise); (vi) under Art. 18(1), where the plaintiff qualifies as a "consumer" according to the criteria listed in the Regulation itself, in the Member State of his or her domicile; and (vii) in matters relating to individual contracts of employment, in the courts for the place where or from where the employee habitually carries out his/her work or in the courts for the last place where he/she did (Art. 21(1)(b)(i)), or, if the employee does not or did not habitually carry out his/her work in any one country, in the courts for the place where the business which engaged the employee is or was situated (Art. 21(1)(b)(ii).

As a matter of fact, a great part of CJEU's case-law pertains to the adaptation of EU's rules on jurisdiction to the online context,[72] with particular regards to the

---

protection and European private international law: Observing a bull in a China shop, International Data Privacy Law, Vol. 5, No. 4, 2015, pp. 261–271.

68 While the domicile of natural persons is defined by the national rules of Member States, according to Art. 63 of the Brussels I-*bis* Regulation the domicile of a legal person corresponds – equally – to its statutory seat, its central administration, or its principal place of business.

69 Case C-334/00 *Fonderie Officine Meccaniche Tacconi SpA v Heinrich Wagner Sinto Maschinenfabrik GmbH (HWS)* [2002] ECR I-07357, par. 27.

70 Case C-21/76 *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA* [1976] ECR 01735, par. 19. Moreover, come si preciserà immediatamente, the victim of a personality right infringement may file a claim – under Art. 7(2) – in the Member State where he/she has his/her centre of interests.

71 Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH and Others v X and Société MGN LIMITED* [2011] ECR I-10269 (see *infra*, note 73).

72 See Trooboff, P. D., *Globalization, Personal Jurisdiction and the Internet Responding to the Challenge of Adapting Settled Principles and Precedents*, Collected Courses of the Hague Academy of International

protection of personality rights.[73] In this last regard, the CJEU clarifies that – under Art. 7(2) of the Brussels I-*bis* Regulation – the victim of such infringements may sue the alleged tortfeasor for the entire damage not only in the Member State of the publisher's place of establishment,[74] but also in the Member State where the plaintiff has his or her centre of interests;[75] such place normally corresponds to the habitual residence of the victim, unless other factors, like "the pursuit of a professional activity" in a different Member State, "establish the existence of a particularly close link with that State".[76] The CJEU also clarified that the plaintiff may seek injunctive relief, as well as the rectification and the removal of content placed online, only before a court with jurisdiction to rule on the entire damage.[77]

Law, Vol. 415, 2021, pp. 137–248, and Marongiu Buonaiuti, F., *La giurisdizione nelle controversie relative alle attività on-line*, Diritto Mercato Tecnologia, Special Issue, 2017, pp. 107–117.

73 For a recent overview of CJEU's case-law in this field, see Svantesson, D.J.B.; Revolidis, I., *From eDate to Gtflix: Reflections on CJEU Case Law on Digital Torts under Art. 7(2) of the Brussels Ia Regulation, and How to Move Forward*, in: Alapantas, P.; Anthimos, A.; Arvanitakis, P. (eds.), National and International Legal Space - The Contribution of Prof. Konstantinos Kerameus in International Civil Procedure, Athens, 2022, pp. 319–371. On this topic, see also Márton, E., *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*, Baden-Baden, 2016. The importance of PIL in regulating online infringements of personality rights has been also recalled at the international level by the Institut de Droit International (IDI), which highlighted the regulatory role ofPIL in this field in its 2019 resolution (Institut de Droit International, Resolution on Internet and the Infringement of Privacy: Issues of Jurisdiction, Applicable Law and Enforcement of Foreign Judgments, 2019 (2019 IDI Resolution) [https://www.idi-iil.org/fr/publications-par-categorie/resolutions/], Accessed 24 July 2023).

74 Case C-68/93 *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-00415, par. 25; conversely, according to the "mosaic principle", "the courts of each Contracting State in which the defamatory publication was distributed and in which the victim claims to have suffered injury to his reputation have jurisdiction to rule on the injury caused in that State to the victim's reputation" (par. 30).

75 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 48. In the CJEU's view, this additional ground of jurisdiction not only benefits the plaintiff, but it is al-so predictable for the defendant (par.50), as long as the connection between the dispute and the courts of the centre of the interests of the alleged victim is based "not on exclusively subjective factors, relating solely to the individual sensitivity of that person, but on objective and verifiable elements which make it possible to identify, directly or indirectly, that person as an individual" (Case C-800/19 *Mittelbayerischer Verlag KG v SM* [2021] not yet published, paras. 41–43).

76 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 49. The CJEU also clarified that the centre of interests for a legal person is in the Member State where "its commercial reputation is most firmly established and must, therefore, be determined by reference to the place where it carries out the main part of its economic activities"; such place may coincide or not with the Member State where the legal person has is registered office (Case C-194/16 *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* [2017] published in the electronic Report of Cases, par. 41).

77 Case C-251/20 *Gtflix Tv v DR* [2021] not yet published, par. 43, where the Court, besides confirming the solution adopted in *Bolagsupplysningen*, (acritically) upheld the mosaic approach, stating that the plaintiff "may claim, before the courts of each Member State in which those comments are or were accessible, compensation for the damage suffered in the Member State of the court seised, even though

This solution is consistent not only with the ubiquitous nature of the information and content placed online,[78] but also with the need to prevent abusive forum and law shopping,[79] especially given that the Rome II Regulation[80] does not apply to "non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation".[81]

The solution adopted in *eDate* is an important example of how some of the rules of the Brussels I-*bis* can be adapted to the online context; nonetheless, such case-law pertains to the infringement of personality rights (which are constitutionally protected), and thus it cannot be automatically transposed to every kind of on-line activities.[82] Accordingly, in several occasions the CJEU clarified that – in the context of online infringements – the place of damage "may vary according to the nature of the right allegedly infringed",[83] and that the *e-Date* approach cannot be extended to any kind of online infringements, even when such infringements produce "dematerialised" damages.[84]

Although the Brussels I-*bis* Regulation provides several heads of jurisdiction, they are normally available only against EU-based controllers or processors. Indeed, according to Art. 5(1), the Regulation normally applies when the defendant is domiciled in a Member State, while, under Art. 6(1), national rules on jurisdiction apply with regard to claims against non-EU defendants. Nonetheless, some of the uniform rules of the Regulation apply irrespective of the defendant's domicile;[85]

---

those courts do not have jurisdiction to rule on the application for rectification and removal". For a critical assessment of the *Gtflix Tv* judgment, see, *inter alia*, Marongiu Buonaiuti, F., *Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet: The Persistence of the Mosaic Approach*, European Papers, Vol. 7, No. 1, 2022, pp. 345–360.

78 Case C-194/16 *Bolagsupplysningen*, note 76, par. 48.

79 See Zarra, G., *Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet*, Rivista di diritto internazionale, Vol. 98, No. 4, 2015, pp. 1242–1243.

80 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199/40 (Rome II Regulation).

81 Art. 1(2)(g) of the Rome II Regulation.

82 See Hess, B., *The Protection of Privacy in the Case Law of the CJEU*, in: Hess, B.; Mariottini, C. (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments, Farnham, 2015, pp. 95–99.

83 Case C-170/12 *Peter Pinckney v KDG Mediatech AG* [2013] published in the electronic Report of Cases, par. 32.

84 Case C-441/13 *Pez Hejduk contro EnergieAgentur.NRW GmbH* [2015] published in the electronic Report of Cases.

85 Indeed, according to Art. 6(1), "If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Article 18(1), Article 21(2) and Articles 24 and 25, be determined by the law of that Member State".

this is the case, e.g., of the aforementioned Art. 25 and Art. 18(1), as well as of Art. 21(1)(b), which is applicable against non-EU employers according to Art. 21(2).[86]

However, the application of the said EU jurisdictional rules over non-EU defendants requires various degrees of connection to be established between the dispute and the EU's territory. In particular, while a choice of courts agreement in favour of a court of a Member State is admissible even where the proceedings has no particular connections with the European Union, the jurisdiction rule for consumer contract requires some connection. Namely, under Art. 17(1)(c), in order for the consumer to sue the professional in the Member State of his or her domicile, the latter should pursue commercial or professional activities in the forum country or should direct such activities there, provided that the contract falls within the scope of the activities at stake. The contractual consumer jurisdiction is thus defined on the basis of a targeting test, which is intended to benefit the consumer as well as to make the competent forum predictable for the defendant, and which goes in parallel with the one normally employed to define the scope of EU rules against natural persons and undertakings established in a Third State.

Accordingly, the CJEU identified a non-exhaustive list of factors indicating when a professional – who runs his or her activities online – is directing his or her activities to the consumer's domicile. In particular, the CJEU clarified that the mere accessibility of a website from a Member State is not sufficient to conclude that the professional was directing his or her commercial activities to that country, and that other elements should be taken into account, among which: (i) the international nature of the activity; (ii) the use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established; (iii) the mention of telephone numbers with an international code; (iv) outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States; (v) use of a top-level domain name other than that of the Member State in which the trader is established; (vi) and mention of an international clientele composed of customers domiciled in various Member States.[87]

---

[86] See also Art. 20(2) states that where the employer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, the employer shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

[87] Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECR I-12527, par. 93; see also Case C-190/11 *Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi* [2012] published in the electronic Reports of Cases, par. 45, where the Court stated that the consumer protective framework set forth in the Brussels regime does not require the contract between the consumer and the trader to be concluded at a distance, while in Case C-218/12 *Lokman Emrek v Vlado Sabranovic* [2013] published in the electronic Reports of

The case-law of the CJEU thus shows not only that the Brussels regime is adaptable to the online and digital context, but also that the need to balance different policy objectives – such as the need to protect the party who appears to be the weaker, on the one hand, and the need to ensure predictability regarding the competent courts, on the other – might give rise to different solutions, depending on the issue at stake.[88]

3.2. Jurisdiction against non-EU defendant under the GDPR

As already observed, the Brussels I-*bis* Regulation applies to data protection disputes involving private parties. Accordingly, in light of the *eadem ratio*, the "centre of interests" rule developed in the context of online defamation is also relevant with regard to the infringements of data subjects' rights.[89] However, the possibility to rely on the jurisdictional grounds provided under the Brussels I-*bis* Regulation in order to foster the application of EU law in this field depends on the scope of the Regulation itself, which applies – in principle – only when the defendant is domiciled within the EU.[90] This means that the *forum actoris* developed by CJEU for the victims of digital infringements of personalities rights is prevented when the defendant is domiciled outside the Union, and that the possibility for a European data subject to sue a non-EU company in the Union will depend on the private international law rules of his or her Member State.[91]

It appears that these shortcomings were considered in the drafting of the GDPR, as it includes several rules aiming at strengthening the protection of data subjects' rights also from a procedural perspective.

First, the GDPR specifies the remedies that data subjects can invoke when their rights under the Regulation are violated, including the right to receive compensa-

---

Cases, par. 32 the CJEU clarified that a causal link between the means employed to direct the commercial or professional activity to the Member State of the consumer's domicile and the conclusion of the contract with that consumer is not required.

88 See Marongiu Buonaiuti, F., *op.cit.*, note 72, pp. 112–113, confronting the *eDate* solution (enabling the victims of online defamation to sue the alleged tortfeasor before the authorities of his/her centre of interests) with the one adopted in the field of consumer contracts, which requires a much stronger connection between the professional (online) activities and the Member State where the consumer has is domicile.

89 Joined Cases C-509/09 and C-161/10 *eDate*, note 71, par. 52. See also Brkan, M., *op. cit.*, note 67, p. 270.

90 See *supra*, par. 3.1.

91 See Brkan, M., *op. cit.*, note 67, p. 265, asking "whether, in the field of data protection, there should be an exception to this general rule of non-applicability of Regulation 1215/2012 if the defendant is domiciled in a third country in the same way as provided for consumers or employees, which are traditionally regarded as weaker (contractual) parties".

tion from the controller or processor for the material and non-material damage suffered as a result of an infringement of EU data protection law (Art. 82).

Moreover, Art. 80 of the GDPR provides a rule on the right of representation of data subjects, according to which data subjects can mandate a not-for-profit body, organisation or association meeting the listed requirements to exercise the rights referred to in the Regulation, including the right to receive compensation *ex* Art. 82, where provided for by Member State law.[92] This rule appears to reflect the need to strengthen access to justice not only where there is a general lack of knowledge of statutory rights and remedies in a given field (like in the case of data protection),[93] but also where a huge number of violations may arise from the same activities.[94] Under this latter perspective, Art. 80 of the GDPR is consistent with both the level of protection accorded by the CJEU[95] and some initiatives of the EU legislature, namely with the Representative Actions Directive, which provides minimum standards for procedural rules on collective redress and injunction for consumers.[96]

In addition, the GDPR sets out two rules on international jurisdiction, as a reaction to the intrinsic cross-border nature of the activities (and infringements) taking place on the Internet. The policy underlying the adoption of specific rules

---

92 Since the right to mandate data subject's right to compensation can be exercised only where Member State law provides for it, the GDPR does not set forth a general right in this sense, to such an extent that the possibility to rely on this peculiar tool will vary among Member States.

93 See the report published by FRA, *Access to data protection remedies in EU Member States*, 2013, [https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states], Accessed 24 July 2023, *passim*, which underlines the need to raise awareness on data protection violations as a first step to ensure access to remedies. On this point, see Gonzáles Fuster, G., *Article 80. Representation of data subjects*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1143–1144.

94 On this topic, see Jančiūtė, L., *Data protection and the construction of collective redress in Europe: Exploring challenges and opportunities*, International Data Privacy Law, Vol. 9, No. 1, 2018, pp. 2–14. As an example of the collective feature of this kind of claims, see the CJEU judgment in the Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] published in the electronic Reports of Cases. At the national level, see Cases C/13/702849, C/13/706680, C/13/706842 *Stichting Onderzoek Marktinformatie et al. v TikTok et al.* [2022] Amsterdam District Court; on this topic, see Silva de Freitas, E.; Kramer, X., *First strike in a Dutch TikTok class action on privacy violation: court accepts international jurisdiction*, 2022, [https://conflictoflaws.net/], Accessed 24 July 2023.

95 Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] published in the electronic Reports of Cases, par. 63.

96 Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1 (Representative Actions Directive). On this topic, see Agulló Agulló, D., *La interacción entre las normas de protección de datos, de defensa de las personas consumidoras y de Derecho internacional privado en el ámbito del acceso colectivo a la justicia en la Unión Europea*, Cuadernos de Derecho Transnacional, Vol. 14, No 2, 2022, pp. 71–91.

on jurisdiction in this field is to protect the data subject also from a procedural perspective.[97] As a matter of fact, Art. 79(2) of the GDPR states that proceedings against a controller or a processor shall be brought: (i) before the courts of the Member State where the controller or processor has an establishment; or (ii) before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority acting in the exercise of its public powers.

Since one of the main objectives underlying the adoption of the GDPR is the protection of fundamental rights, it appears that the European legislature has adopted a *forum actoris* that resembles the one developed in *eDate*, but whose application is not limited to proceedings against non-EU defendant.[98] As a matter of fact, Art. 79(2) strengthen the protection of data subjects not only because it enables them to seise their "home court", but also because it support the "extra-territorial" and coherent application of EU rules by ensuring equal access to justice against non-EU controller/processors.[99]

Since the availability of multiple fora may give rise to multiple proceedings against the same controller or processor, the Regulation also provides a mechanism for cases where several proceedings "concerning the same subject matter as regards processing by the same controller or processor" are pending before the authorities of different Member States,[100] even though – in light of Recital 144 of the GDPR – it appears that such rule applies only to proceedings against a decision issued by supervisory authority, and not when proceedings in civil and commercial matters are pending in several Member States.[101]

As private claims against controllers or processors normally relate to civil and commercial matters, problems of coordination between the jurisdictional grounds set forth in Art. 79(2) of the GDPR and those of the aforementioned Brussels I-*bis* Regulation may arise.[102] The relationship between the two instruments is tackled

---

97 See Franzina, P., *op. cit.*, note 66, pp. 97–98.

98 De Miguel Asensio, P., *op. cit.*, note 15, p. 159.

99 In this regard, see Art. 27(5) of the GDPR, requiring non-EU controllers or processors that are within the scope of the Regulation according to Art. 3(2) to designate a representative in the Union, with the clarification that such designation "shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves".

100 Art. 81 of the GDPR. However, scholars have pointed out that this provision is "less sophisticated" than the general regime laid down in Art. 29 and Art. 30 of the Brussels I-*bis* Regulation. In this regard, see Franzina, P., *op. cit.*, note 66, p. 106.

101 *Ibid.*, pp. 105–106; see also De Miguel Asensio, P., *op. cit.*, note 15, pp. 162–163.

102 On this topic, see also Marongiu Buonaiuti, F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina conte-*

in Recital 147 of the GDPR, which clarifies that "(w)here specific rules on jurisdiction are contained in this Regulation (…), general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules". This solution is consistent with Art. 67 of the Brussels I-*bis* Regulation, according to which the Regulation does not prejudice the application of provisions governing jurisdiction in specific matters which are contained in other EU instruments, like those laid down in Art. 79(2) of the GDPR. Thus, the coordinated reading of the two provisions appears to suggest the prevalence of the jurisdictional rules set forth in the GDPR, which are *leges speciales* in disputes initiated against controllers/processors for infringements of the right to data protection.[103] This conclusion is also confirmed by Recital 145 of the GDPR, underlining that the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides.

Even though Art. 79(2) of the GDPR is specifically designed for claims in the field of data protection (and in this sense it "prevails" on the rules laid down in the Brussels I-*bis* Regulation), it is not exclusive in nature. This means that the jurisdictional grounds set forth in the GDPR are additional, and that the rules of the Brussels I-*bis* Regulation continue to apply as long as their application is compatible with EU data protection law. Accordingly, the possibility for the plaintiff to rely on Art. 79(2) of the GDPR cannot be impaired by the application of Brussels I-*bis* Regulation's rules, as in the case where an exclusive prorogation agreement concluded between the data subject and the controller or processor exists. Nonetheless, such rules are still applicable where they expand the range of possible *fora* in favour of the plaintiff.[104]

Thus, the question arise whether the jurisdiction rules of the Brussels I-*bis* Regulation, where applied in the context of data protection infringements, are in practice capable of enlarging the possibilities provided by Art. 79(2) of the GDPR.[105] In particular, the Member State where the controller or processor has an establishment for the purpose of Art. 79(2) of the GDPR will normally correspond

nuta nel regolamento "Bruxelles I-bis", Cuadernos de Derecho Transnacional, Vol. 9, No. 2, 2017, pp. 448–464.

103 Kotschy, W., *Article 79. Right to have an effective remedy against a controller or processor*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, p. 1137.

104 Kohler, C., *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, Rivista di diritto internazionale privato e processuale, Vol. 52, No. 3, 2016, p. 669. For an in-depth analysis of the coordination of Art. 79(2) of the GDPR and the Brussels I-*bis* Regulation, see Franzina, P., *op. cit.*, note 66, pp. 103–108.

105 Kohler, C., *op. cit.*, note 104, pp. 669–670.

to the place where the defendant is domiciled under Art. 4 of the Brussels I-*bis* Regulation,[106] and the *forum delicti* according to Art. 7(2) of the Brussels I-*bis* Regulation, as interpreted by the CJEU,[107] may frequently coincide with the data subject's habitual residence.[108] Moreover, if the processing of personal data is connected to a contract between the data subject and the defendant, the plaintiff could also rely on the *forum contractus* under Art. 7(1) of the Brussels I-*bis* Regulation, and – where the criteria listed in Art. 17(1)(c) are met – on the consumer jurisdiction rule set forth in Art. 18(1). Once again, this last ground for jurisdiction may most likely coincide with the habitual residence of data subject in the sense of Art. 79(2) of the GDPR.

As already mentioned, when the defendant is not domiciled in the EU, the uniform jurisdiction rules under Brussels I-*bis* Regulation (generally) does not apply. By contrast, the rule on jurisdiction included in the second indent of Art. 79(2) of the GDPR is designed to apply also against controllers or processors not established in the EU. Accordingly, also national rules on jurisdiction – which have been incorporated into EU law by means of the aforementioned Art. 6(1) of the Brussels I-*bis* Regulation[109] – shall not prejudice the application of the jurisdiction rules set forth in the GDPR.[110]

3.3. EU's approach to Artificial Intelligence and PIL issues: the lack of specific rules on jurisdiction

In light of the role played by civil liability in balancing the protection of victims of AI-related harms with the need to promote digital innovation within the EU,[111] scholars highlighted the role of PIL in regulating AI in a cross-border context.[112] Nonetheless, the (proposed) legislation does not explicitly refers to private international law issues, and it only declares the application of EU rules within its own territorial scope, to such an extent that EU rules in this field operate as "unilateral conflict rules". Accordingly, the instruments at stake aim at applying to

---

106 Franzina, P., *op. cit.*, note 66, p. 104.

107 See par. 3.2. of this paper.

108 De Miguel Asensio, P., *op. cit.*, note 15, pp. 159–160.

109 Opinion of the CJEU No 1/03 on the competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] ECR I-01145, paras. 144–148.

110 De Miguel Asensio, P., *op. cit.*, note 15, p. 159.

111 Recital B of the AI Liability Regime Resolution.

112 See, in particular, Poesen, M., *op.cit.*, note 46. See also Wagner, G., *Liability for Artificial Intelligence: A Proposal of the European Parliament*, 14 July 2021, pp. 25–26 [Available at SSRN: https://ssrn.com/abstract=3886294 or http://dx.doi.org/10.2139/ssrn.3886294].

the relationships that are within their scope irrespective of the law designated as applicable under the Rome II Regulation.

Where analysed through the prism of PIL, it appears that such substantive rules are not always capable to properly reflect the relevant EU policy in AI matters. This is particularly evident when it comes to the proposal for Regulation attached to the EU Parliament's Recommendation, whose territorial scope reflected the *lex loci damni* approach.[113] It has been pointed out that this solution – according to which the proposed Regulation should apply every time an AI-system causes harms or damages within the territory of the Union – is questionable, among other things, because it resembles the general conflict-of-laws rule for torts envisaged by Rome II Regulation (Art. 4), and it does not appear to be consistent with the special rule for cases relating to product liability (Art. 5).[114]

Recital 20 of the Rome II Regulation underlines that "(t)he conflict-of-law rule in matters of product liability should meet the objectives of fairly spreading the risks inherent in a modern high-technology society, protecting consumers' health, stimulating innovation, securing undistorted competition and facilitating trade". Accordingly, Art. 5 provides a solution which is more "victim friendly" than the one envisaged in Art. 4,[115] since it establishes a cascade system of connecting factors that privilege proximity with the person sustaining the damage, but also predictability for the person claimed to be liable. Then, although the purposes recalled in the aforementioned Recital 20 are similar to those underlying the proposed framework in the field of AI liability, the EU Parliament Recommendation adopted a solution which is less "sophisticated" than that enshrined in the Rome II Regulation, as it deploys an approach that appear to be overly simplistic, especially in the light of the specific feature of AI-related harms.[116]

---

113 Art. 2(1) of the Regulation Proposal attached to the AI Liability Regime Resolution.

114 This rule establishes a cascade system of connecting factors, with the first of them being the law of the country where the victim has his or her habitual residence when the damage occurred, provided that the product was marketed there (Art. 5(1)(a)); whether this criterion could not be used, the law of the country in which the product was acquired should apply (Art. 5(1)(b)); failing that, the applicable law should be the law of the country in which the damage occurred (Art. 5(1)(c). Also these two latter criteria apply provided that the product was marketed in those countries.

115 See von Hein, J., *Forward to the Past: A Critical Note on the European Parliament's Approach to Artificial Intelligence in Private International Law*, 22 October 2020 [https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to-artificial-intelligence-in-private-international-law/] Accessed 24 July 2023.

116 *Ibid*. See also Poesen, M., *op. cit.*, note 46, par. II.2, pointing out that "the place-of-injury rule burdens those whose behaviour may incur liability", as the applicable law may not always be foreseeable, and that, in conclusion, "the Parliament Recommendations have not seized the opportunity to open the debate about the role of EU PrIL in regulating AI".

Disconnections have also been underlined between the EU Parliament's approach and Art. 14 of the Rome II Regulation. In fact, Art. 2(2) of the proposal attached to the EU Parliament Recommendation aimed at enhancing the protection of AI-users by limiting the autonomy of the parties. More specifically, the rule intended to bar the possibility for the operator of an AI-system to conclude (before or after the harm or damage occurred) an agreement with the victim, in order to circumvent or limit the rights and obligations set out in the proposed Regulation. Where adopted, this proposal would be in strong conflict with the rationale underlying EU's liberal approach in private international law, as the possibility for the parties to select freely the law governing their relationships is the cornerstone of EU PIL, not only in contractual matters (Art. 3 of Rome I Regulation), but also in non-contractual matters.[117]

Even considering EU rules on AI liability as unilateral conflict rules", their effective application may be pacifically ensured only before a court in the EU. Since there are no indications regarding the issue of international jurisdiction, claims within the scope of the proposed instruments will be regulated under the Brussels I-*bis* Regulation, and namely under Art.7(2), which – albeit not shaped in order to tackle AI-related harms – appear to be suited to the emerging framework on AI and civil liability.

In particular, and as long as liability for defective products is concerned, it appears to be relevant the solution adopted in *Zuid-Chemie*, where the CJEU specified that the place where the damage occurred is the place where the damage caused by the defective product actually manifests itself; therefore, it must not be confused with the place where the event which damaged the product itself occurred, which corresponds to the place of the event giving rise to the damage.[118] In the same occasion, the CJEU also clarified that Art. 7(2) designates "the place where the initial damage occurred as a result of the normal use of the product for the purpose for which it was intended".[119]

As observed above, the proposed amendments to the Product Liability Directive take "into account the growing significance of products manufactured outside the Union, and ensures that there is always an economic operator in the Union against

117 See von Hein, J., *op.cit.*, note 115.

118 Case C-189/08 *Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA.* [2009] ECR I-06917, par. 27. With regard to the applicability of the solution developed in *Zuid-Chemie* in the field of AI-related harms, see Cappiello, B., *AI-systems and non-contractual liability. A European private international law analysis*, Torino, 2022, p. 176, according to whom AI-related harms "fit within the solution already provided for by the ECJ", to such an extent that "a special head for jurisdiction for AI-systems would be superfluous".

119 Case C-189/08 *Zuid-Chemie BV*, note 118, par. 32.

whom a compensation claim can be made".[120] Accordingly, the issue of jurisdiction against non-EU operator appears to be less of an urgent point in this field, as Art. 7(2) of the Brussels I-*bis* Regulation may apply in a wide range of cases.

However, the lack of provisions concerning private international law raises few concerns in all those cases that – although related to damages caused by AI-systems – may fall outside the scope of the Product Liability Directive.

First, it is not consistent with the solution adopted in the GDPR, which incorporates a specific set of rules on jurisdiction in order to support the effective (and in some way "extraterritorial") application of the Regulation. Moreover, jurisdiction against defendants established in Third States will be mostly assessed in the light of the national rules of the Member States, which may not always be capable to attract this kind of proceedings before a court in the EU, and which – in light of the differences among national laws – do not ensure the victims of AI-related torts equal access to justice. As a consequence, it appears that there is a degree of uncertainty with regard to the concrete application of EU rules in the field of AI-systems, at least in cases related to non-EU States.

3.4. The issue of jurisdiction in the Online Platform Regulation and in the Platform Workers Directive Proposal

Even though the Online Platform Regulation aims at applying in broad terms (and with the specific objective of making redress possibilities accessible to business users of online platforms), the European legislature did not provide for a complete set of procedural provisions specifically designed to ensure its effective application world-wide. Indeed, unlike the GDPR, the Online Platform Regulation does not enshrine rules on international jurisdiction, and the only procedural tool set out in the instrument concerns the right of action of organisations and associations having a legitimate interest in representing business users (Art. 14), which resembles the aforementioned Art. 80 of the GDPR.

In the lack of specific jurisdiction rules, the Brussels I-*bis* Regulation applies with regard to the situations covered by the Online Platform Regulation. Accordingly, notwithstanding the general competence of the court of the Member State where the defendant has his or her domicile, jurisdiction against EU-based platform operator may be conferred, in contractual matters, pursuant to Art. 7(1)(b), and, in matters relating to torts, pursuant to Art. 7(2).[121] Therefore, absent a choice-

[120] See the explanatory memorandum attached to the Proposal, p. 12.

[121] For disputes arising out of the operations of a branch, agency or other establishment, the claimant has also the opportunity to sue the platform operator in the courts for the place where the branch, agency

of-court agreement conferring jurisdiction on a court in the EU under Art. 25 of the Brussels I-*bis* Regulation (as well as a tacit prorogation *ex* Art. 26), jurisdiction against non-EU domiciled defendants is regulated, in principle, according to the internal rules of the Member States. This circumstance does not ensure equal access to justice for European businesses, since national rules vary – quite consistently in some cases – from one Member State to another.[122] As a consequence, EU claimants will be able to litigate in their home country only if they are domiciled[123] in a Member State that employs a jurisdictional ground enabling them to do so, i.e. the nationality of the plaintiff.[124]

The absence of a specific set of jurisdiction rules in the Online Platform Regulation, designed to support its application against defendant established in Third States, is even more surprising if one considers that the substantive rules contained therein appears to qualify as "overriding mandatory provisions" pursuant to Art. 9 of the Rome I Regulation and Art. 16 of the Rome II Regulation.[125] The effective application of such mandatory rules may indeed be unproblematic only when claims are heard by a court in the EU. In the absence of uniform EU rules suited to assert jurisdiction over defendants domiciled in Third States, proceedings involving non-EU platform operators may be attracted before foreign courts that apply conflict-of-laws rules that do not guarantee the application of the Regulation's provisions.[126]

The same line of reasoning is applicable to the Platform Workers Directive Proposal. In fact, and in order for the instrument to be effective, the Proposal requires Member States to ensure that platform workers – both individually and collectively – "have access to effective and impartial dispute resolution and a right to redress, including adequate compensation, in the case of infringements of their rights arising from this Directive" (Art. 13 and Art. 14). Then, since the rights and

---

or other establishment is situated, under Art. 7(5).

122 See Nuyts, A., *Study on residual jurisdiction. General report*, 3 September 2007, [https://gavclaw.files.wordpress.com/2020/05/arnaud-nuyts-study_residual_jurisdiction_en.pdf], Accessed 24 July 2023.

123 Indeed, according to Art. 6(2) of the Brussels I-*bis* Regulation, "any person domiciled in a Member State may, whatever his nationality, avail himself in that Member State of the rules of jurisdiction there in force".

124 See Franzina, P., *Promoting Fairness and Transparency for Business Users of Online Platform: The Role of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018,, p. 156.

125 *Ibid.*, p. 151.

126 *Ibid.*, pp. 152–153, that highlights that, except where – according to the conflict-of-laws rules applied by a foreign court – the relationship is governed by the law of a Member State, the rules of the Online Platform Regulation "would in fact be regarded as overriding mandatory provisions of a legal system which is neither the *lex fori* nor the *lex cause*…".

obligations enshrined in the Directive Proposal also apply to Platforms established outside the EU, as long as they organise work performed in the Union, Member States' obligation to ensure access to redress mechanisms includes claims against non-EU platforms. Nonetheless, the Proposal does not provide any provision in the field of PIL: once again, jurisdiction in cases involving non-EU actors may mostly fall under the Brussels I-*bis* Regulation.

In particular, claims concerning rights set forth in the Directive may fall – in a number of cases – under the protective rules designed for individual contracts of employment, that, among other things, enable employees to sue employers – irrespective of their place of establishment[127] – in the Member State where or from where the employees habitually carries out their work or in the last Member State where they did so (Art. 21(1)(b)(i)). Moreover, according to the protective framework regarding employment matters, a choice-of-court agreement in this matter is admissible only if it is entered into after the dispute has arisen or if it allows the employee to bring proceedings in courts other than those indicated in the Section 5 of the Regulation,[128] thus enlarging the opportunities for the employee to sue the employer before a (different) court in the EU.

In this last regard, the CJEU clarified that, although the Brussels regime does not directly address the issue of choice-of-courts agreements conferring jurisdiction on a court in a Third State,[129] such an agreement is admissible only if it is not "exclusive" in nature, i.e. if it does not prohibit the employee from bringing proceedings before the courts which have jurisdiction under Art. 20 and 21 of the Brussels I-*bis* Regulation.[130] Nonetheless, it is open to question whether this solution is specific

127 See Art. 21(2) of the Brussels I-*bis* Regulation.

128 See Art. 23 of the Brussels I-*bis* Regulation.

129 Suffice it to observe that the enforceability of an agreement conferring jurisdiction on the courts of non-EU countries will mostly fall within the scope of the 2007 Lugano Convention (Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2007] OJ L 339/3) or within the scope of the 2005 Hague Convention (Hague Convention on Choice of Court Agreements, concluded on 30 June 2005, entered into force on 1 October 2015), and that, according to the Conventions at stake, judges in the EU might be required to decline their jurisdiction even when, in doing so, the effective application of EU law would be undermined. In this regard, see Franzina, P., *op. cit.*, note 124, p. 157, observing that is open to question whether, in such cases, the enforceability of the choice-of-court agreement might be precluded according to Art. 6(c) of the 2005 Hague Convention, which states that "A court of a Contracting State other than that of the chosen court shall suspend or dismiss proceedings to which an exclusive choice of court agreement applies unless… giving effect to the agreement would lead to a manifest injustice or would be manifestly contrary to the public policy of the State of the court seised".

130 Case C-154/11 *Ahmed Mahamdia v République algérienne démocratique et populaire* [2012] published in the electronic Report of Cases, paras. 61–66). On this topic, see Villata, F. C., *L'attuazione degli accordi di scelta del foro nel regolamento Bruxelles I*, Cedam, Padova, 2012, pp. 199–254.

for claims regarding employment matters (and might theoretically be extended to other cases for which the Brussels I-*bis* regulation prescribes protective rules), or if instead it might be adopted as a general solution.[131] In the latter case, the solution adopted in *Mahamdia* would prevent jurisdiction before a court in the EU to be barred, for example, when service providers operating within the scope of the Online Platform Regulation include in their terms and conditions an exclusive choice-of-court clause designating a court in a Third State.[132]

Finally, since platform work can blur the boundaries between employment relationship and self-employed activity,[133] it might be questionable whether the protective rules provided in the Brussels regime are accessible to any platform worker. Even though the Brussels I-*bis* Regulation does not provide any definition of "contract of employment", the CJEU clarified that it is an independent concept, which "create a lasting bond which brings the worker to some extent within the organisational framework of the business of the undertaking or employer… in return for which he [or she] received remuneration".[134] Thus, the question is whether such definition is sufficient to preclude that the features of platform work give rise to misclassification of the employment status, in order to preclude the workers' access to protective *fora*. In the event of the disconnection within the definition provided by the CJEU and the characteristics of platform work, workers may not be able to rely on the protective rules set forth in the Regulation, which are also applicable against employers that are not established in the EU. As a consequence, in this kind of proceedings, jurisdiction against non-EU platforms may be assessed in light of the residual application of national rules on jurisdiction: this solution does not ensure equal access to justice for EU workers.

This is even more problematic if one considers that the obligation set forth in Art. 13 should not affect the application of Art. 79 and Art. 82 of the GDPR. This means that, where a worker's rights under the Directive Proposal are infringed by means of activities that are partially related to the processing of his or her personal data, claims pertaining to privacy infringements may be regulated according to EU jurisdiction rules (namely through Art. 79(2) of the GDPR), while jurisdic-

131 See Magnus, U., *Article 25*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 604–605.

132 See Franzina, P., *op. cit.*, note 124, p. 158.

133 See note 63.

134 See, *inter alia*, Case C-47/14 *Holterman Ferho Exploitatie BV et al. v F.L.F. Spies von Büllesheim* [2015] published in the electronic Report of Cases, paras. 39–45. On this point, see Esplugues Mota, C.; Palao Moreno, G., *Article 20*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 539–540.

tion over claims not related to the misuse of personal data could be assessed in the light of Member States national rules.

4. CONCLUSIONS

In light of the pivotal role that new technologies play for the achievement of policy objectives, and considering their ability to negatively affect rights and freedoms in a ubiquitous manner, the EU is adopting a number of instruments to regulate those matters that are particularly affected by digitalisation, especially (but not only) in the field of personality rights. Indeed, this legislation aims at regulating the usage of digital technologies in order to ensure the proper functioning of the internal market, as well as the protection of the rights recognised under EU law, even when digital activities take place abroad.

Accordingly, some recent EU acts and proposals in this field define their own territorial scope in a broad way and by means of "unilateral conflict rules" that are meant to prevail over the application of conflict-of-laws rules enshrined in Rome I and Rome II Regulation. Nonetheless, it appears that limited attention is generally paid to other issues in the field of PIL. In particular, even though such instruments are aimed at applying outside the EU borders, they do not usually provide special provisions on international jurisdiction supporting the "extraterritorial" application of EU substantive rules.

This is rather counterintuitive, if one considers that – in other occasions – EU acts in this field have been equipped with special grounds for jurisdiction, suited to support such broad application. This is the case of Art. 79(2) of the GDPR, providing that proceedings against the controller or the processor of personal data may be brought not only before the court of the Member State where the controller or processor has an establishment, but also before the court of the Member State where the user has his or her habitual residence, the latter ground being suitable also for claims against non-EU domiciled defendants.

In the absence of special jurisdiction rules within the context of other EU instruments – i.e. the Online Platforms Regulation and several proposals in the field of digital technologies –, the Brussels I-*bis* Regulation may apply in the event of cross-border infringements of the rights enshrined in such legislation. This circumstance is open to criticisms. In the first place, EU rules on jurisdiction in civil and commercial matters were not drafted in light of the characteristics of digitalisation. Accordingly, they have been progressively interpreted in order to tackle the issue of infringements related to the use of technologies. Nonetheless, whether the CJEU will be able to adapt – under all circumstances – EU jurisdiction rules to

the lack of jurisdictional grounds suited to digital infringements is open to question. Moreover, the Brussels I-*bis* Regulation normally applies where the defendant is domiciled within the European Union, and only a limited number of EU jurisdiction rules applies to non-EU domiciled defendants. Even if some of these latter rules appear to be relevant within the context of claims in digital matters, a number of cases may fall within the scope of the residual application of Member States' national rules on jurisdiction. This appears to be problematic, since persons located in the EU may not have equal access to justice in the EU to enforce their rights against non-EU actors.

This circumstance also ends up affecting the role of the EU as a "global regulator" in the digital field. In fact, although the EU aims at projecting its digital policies abroad by adopting instruments with a broad territorial scope, the concrete application of EU rules outside EU borders will mostly depend on the existence, within the national rules of the Member States, of jurisdiction rules suited to attract this kind of proceedings before a court in the European Union. Accordingly, in order for the EU to improve its regulatory power, a number of solutions might be considered.

A first approach would consist in equipping EU substantive legislation in digital matters with jurisdiction rules suited to support their "extraterritorial" application, in the vein of Art. 79(2) of the GDPR. Nevertheless, the framework set up in the GDPR could only partially represent a valid model of how the interplay between the extraterritorial application of EU substantive rules and the rules on jurisdiction should work. As a matter of fact, the adoption of special jurisdictional grounds does not ensure, *per se*, the achievement of such result. Thus, a number of other actions should be taken, especially with regard to parallel proceedings and recognition and enforcement of judgments issued by courts in Third States.

Another possible solution would consist in emending the Brussels I-*bis* Regulation, in order to make (at least some of) its jurisdiction rules applicable against non-EU defendants. In particular, enlarging the scope of application of the aforementioned Art. 7(1) and Art. 7(5) would be a valid solution,[135] even for proceedings pertaining to digital matters. Extending the former would allow an EU actor (that is not a consumer) to sue a non-EU party before a court in a Member State, as long as the defendant directs his or her activities to the internal market; extending the latter would consent to consider a non-EU company that has a branch in a Member State as domiciled in the Union, at least with regard to disputes arising

[135] On the opportunity to extend these two heads of jurisdiction to non-EU defendants, see Hess, B., *et al.*, *The Reform of the Brussels Ibis Regulation*, MPILux Research Paper Series, No. 6, 2022 [Available at SSRN: https://ssrn.com/abstract=4278741 or http://dx.doi.org/10.2139/ssrn.4278741], pp. 15–16.

out of the operations of such branch. Conversely, a general extension of Art. 7(2) to non-EU defendants would be more problematic in terms of predictability.[136]

A better approach would thus consist in adopting special heads of jurisdiction reflecting the policies of the EU in digital matters. In particular, in light of the need to ensure the concrete projection of EU digital values abroad, such rules could be designed in the same vein of the protective rules that are already enshrined within the Brussels I-*bis* Regulation, with regard to the so-called "weaker parties".[137] In fact, since digital technologies have the ability to seriously affect individuals, their use in certain contexts could result in the creation of new categories of protective grounds for jurisdiction, aimed at conferring benefits in terms of access to courts upon the victims of digital infringements.[138] Moreover, this solution appears to be consistent with the case-law of the CJEU pertaining to online defamation, where the Court creates a *forum actoris* that ensure the defamed person the possibility to claim compensation for the entire damage in the Member State where he or she has is habitual residence.

Under this perspective, a sectorial approach should thus be preferred to the reform of the Brussels I-*bis* Regulation, at least as long as digital matters are involved. Indeed, a similar solution would permit to select the situations for which the creation of similar protective grounds is needed, and it would also allow for better shaping the terms of the intervention of the European legislature in this field.

REFERENCES

BOOKS AND ARTICLES

1. Agulló Agulló, D., *La interacción entre las normas de protección de datos, de defensa de las personas consumidoras y de Derecho internacional privado en el ámbito del acceso colectivo a la justicia en la Unión Europea*, Cuadernos de Derecho Transnacional, Vol. 14, No 2, 2022, pp. 71–91
2. Bradford, A., *The Brussels Effect: How the European Union Rules the World*, New York, 2020
3. Brkan, M., *Data protection and European private international law: Observing a bull in a China shop*, International Data Privacy Law, Vol. 5, No. 4, 2015, pp. 257–278

136 *Ibid*., p. 16.

137 In this regard, and in relation to platform users within the context of the Online Platform Regulation, see Franzina, P., *op. cit.*, note 124, p. 160.

138 See also Brkan, M., *op. cit.*, note 67, p. 265, stating that enlarging the scope of the Brussels I-*bis* Regulation to non-EU defendants in the field of data protection 'would not only be beneficial for European data subjects, but it would also strike a fair balance between different positions of a stronger controller and a weaker data subject, regardless of whether data are processed on a contractual basis or not'.

4. Cappiello, B., *AI-systems and non-contractual liability. A European private international law analysis*, Torino, 2022
5. Chamberlain, J., *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, European Journal of Risk Regulation, Vol. 14, No. 1, 2023, pp. 1–13
6. Chia, C. W., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, Singapore Academy of Law Journal, Vol. 30, No. 2, 2018, pp. 833–870
7. Cremona, M.; Scott, J. (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford, 2019
8. De Miguel Asensio, P., *Conflict of Laws and the Internet*, Cheltenham and Northampton, 2020
9. Esplugues Mota, C.; Palao Moreno, G., *Article 20*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 537–543
10. Franzina, P., *Promoting Fairness and Transparency for Business Users of Online Platform: The Role of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 147–162
11. Franzina, P., *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in: De Franceschi, A. (ed.), European Contract Law and the Digital Single Market. The Implications of the Digital Revolution, Cambridge, 2017, pp. 81–108
12. Gonzáles Fuster, G., *Article 80. Representation of data subjects*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1142–1152
13. de Hert, P.; Czerniawski, M., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Vol. 6, No. 3, 2016, pp. 230–243
14. Hess, B., *et al.*, *The Reform of the Brussels Ibis Regulation*, MPILux Research Paper Series, No. 6, 2022 [Available at SSRN: https://ssrn.com/abstract=4278741 or http://dx.doi.org/10.2139/ssrn.4278741]
15. Hess, B., *The Protection of Privacy in the Case Law of the CJEU*, in: Hess, B.; Mariottini, C. (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments, Farnham, 2015, pp. 81–113
16. Hustinx, P., *EU Data Protection Law: The Review of Directive 95/46/CE and the General Data Protection Regulation*, in: Cremona, M. (ed.), New Technologies and EU Law, Oxford, 2017, pp. 123–173
17. Jančiūtė, L., *Data protection and the construction of collective redress in Europe: Exploring challenges and opportunities*, International Data Privacy Law, Vol. 9, No. 1, 2018, pp. 2–14
18. Kohler, C., *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, Rivista di diritto internazionale privato e processuale, Vol. 52, No. 3, 2016, pp. 653–675

19. Kotschy, W., *Article 79. Right to have an effective remedy against a controller or processor*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 1132–1141
20. Lutzi, T., *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in: Pretelli, I. (eds.), Conflict of Laws in the Maze of Digital Platforms/ Le Droit International Privé Dans le Labyrinthe des Plateformes Digitales, Zürich, 2018, pp. 129–145
21. Magnus, U., *Article 25*, in: Magnus, U.; Mankowski, P. (eds.), Brussels Ibis Regulation, Köln, 2023, pp. 580–665
22. Mantovani, M., *Horizontal Conflicts of Member States' GDPR-Complementing Laws: The Quest for a Viable Conflict-of-Laws Solution*, Rivista di diritto internazionale privato e processuale, Vol. 55, No. 3, 2019, pp. 535–562
23. Marongiu Buonaiuti, F., *Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet: The Persistence of the Mosaic Approach*, European Papers, Vol. 7, No. 1, 2022, pp. 345–360
24. Marongiu Buonaiuti, F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis"*, Cuadernos de Derecho Transnacional, Vol. 9, No. 2, 2017, pp. 448–464
25. Marongiu Buonaiuti, F., *La giurisdizione nelle controversie relative alle attività on-line*, Diritto Mercato Tecnologia, Special Issue, 2017, pp. 89–128
26. Márton, E., *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*, Baden-Baden, 2016
27. Moerel, L., *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, International Data Privacy Law, Vol. 1, No. 1, 2011, pp. 28–46
28. Poesen, M., *Regulating Artificial Intelligence (AI) in the European Union (EU): Exploring the Role of Private International Law*, X, Recht in beweging – 29ste VRG-Alumnidag 2022, 2022, pp. 297–314 [Available at SSRN: https://ssrn.com/abstract=3959643 or http://dx.doi.org/10.2139/ssrn.3959643]
29. Pretelli, I., *Protecting Digital Platform Users by Means of Private International Law*, Cuadernos de Derecho Transnacional, Vol. 13, No. 1, 2021, pp. 574–585
30. Requejo Isidro, M., *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection*, MPILux Research Paper Series, No. 3, 2019 [Available at SSRN: https://ssrn.com/abstract=3339180 or http://dx.doi.org/10.2139/ssrn.3339180]
31. Saluzzo, S., *The Principle of Territoriality in EU Data Protection Law*, in: Natoli, T., Riccardi A.(eds.), Borders, Legal Spaces and Territories in Contemporary International Law, Cham, 2019, pp. 121–141
32. Scott, J., *Extraterritoriality and Territorial Extension in EU Law*, The American Journal of Comparative Law, Vol.62, No. 1, 2014, pp. 87–125
33. Svantesson, D.J.B.; Revolidis, I., *From eDate to Gtflix: Reflections on CJEU Case Law on Digital Torts under Art. 7(2) of the Brussels Ia Regulation, and How to Move Forward*, in: Alapantas, P.; Anthimos, A.; Arvanitakis, P. (eds.), National and International Legal Space - The

Contribution of Prof. Konstantinos Kerameus in International Civil Procedure, Athens, 2022, pp. 319–371

34. Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, L. A.; Docksey, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020, pp. 74–99
35. Trooboff, P. D., *Globalization, Personal Jurisdiction and the Internet Responding to the Challenge of Adapting Settled Principles and Precedents*, Collected Courses of the Hague Academy of International Law, Vol. 415, 2021
36. Villata, F. C., *L'attuazione degli accordi di scelta del foro nel regolamento Bruxelles I*, Cedam, Padova, 2012
37. Vogiatzoglou, P., Valcke, P., *Two decades of Article 8 CFR: A critical exploration of the fundamental right to data protection in EU law*, in: Kosta, E.; Kamara, I.; Leenes, R. (eds.), Research Handbook on EU Data Protection Law, Northampton, 2022, pp. 11–49
38. Wagner, G., *Liability for Artificial Intelligence: A Proposal of the European Parliament*, 14 July 2021, pp. 1–36 [Available at SSRN: https://ssrn.com/abstract=3886294 or http://dx.doi.org/10.2139/ssrn.3886294]
39. Zarra, G., *Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet*, Rivista di diritto internazionale, Vol. 98, No. 4, 2015, pp. 1231–1262

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-251/20 Gtflix Tv v DR [2021] not yet published
2. Case C-800/19 Mittelbayerischer Verlag KG v SM [2021] not yet published
3. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] not yet published
4. Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV [2019] published in the electronic Reports of Cases
5. Case C-498/16 Maximilian Schrems v Facebook Ireland Limited [2018] published in the electronic Reports of Cases
6. Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018] published in the electronic Reports of Cases
7. Case C-194/16 Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB [2017] published in the electronic Report of Cases
8. Case C-192/15, T. D. Rease and P. Wullems v College bescherming persoonsgegevens [2015] OJ C78/11
9. Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] published in the electronic Reports of Cases
10. Case C-47/14 Holterman Ferho Exploitatie BV et al. v F.L.F. Spies von Büllesheim [2015] published in the electronic Report of Cases

11. Case C-441/13 Pez Hejduk contro EnergieAgentur.NRW GmbH [2015] published in the electronic Report of Cases
12. Case C-413/13 FNV Kunsten Informatie en Media v Staat der Nederlanden [2014] published in the electronic Reports of Cases
13. Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzále [2014] published in the electronic Reports of Cases Case C-218/12 Lokman Emrek v Vlado Sabranovic [2013] published in the electronic Reports of Cases
14. Case C-170/12 Peter Pinckney v KDG Mediatech AG [2013] published in the electronic Report of Cases
15. Case C-190/11 Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi [2012] published in the electronic Reports of Cases
16. Case C-154/11 Ahmed Mahamdia v République algérienne démocratique et populaire [2012] published in the electronic Report of Cases
17. Joined Cases C-509/09 and C-161/10 eDate Advertising GmbH and Others v X and Société MGN LIMITED [2011] ECR I-10269
18. Joined Cases C-585/08 and C-144/09 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller [2010] ECR I-12527
19. Case C-189/08 Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA. [2009] ECR I-06917
20. Opinion of the CJEU No 1/03 on the competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] ECR I-01145
21. Case C-334/00 Fonderie Officine Meccaniche Tacconi SpA v Heinrich Wagner Sinto Maschinenfabrik GmbH (HWS) [2002] ECR I-07357
22. Case C-68/93 Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA [1995] ECR I-00415
23. Case C-21/76 Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA [1976] ECR 01735

ECHR

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108
2. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11, 14 and 15, 4 November 1950, ETS 5 (ECHR)
3. *Amann v Switzerland* (2000) 30 EHRR 843

EU LAW

1. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules

on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)

2. Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 0836-02/10/EN, WP 179
3. Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (CFREU)
4. Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2007] OJ L 339/3
5. Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29 (Product Liability Directive)
6. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive)
7. Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1 (Representative Actions Directive)
8. European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018 (version 2.1 of 7 January 2020)
9. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) (AI Liability Regime Resolution)
10. General Approach adopted by the Council on 12 June 2023 on the Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work (Document ST_10758_2023_INIT)
11. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (AI Liability Directive Proposal)
12. Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final (Platform Workers Directive Proposal)
13. Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final
14. 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 (AI Act Proposal)
15. Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199/40 (Rome II Regulation)
16. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177/6 (Rome I Regulation)

17. Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351/1 (Brussels I-*bis* Regulation)
18. Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [2016] OJ L 119/1 (General Data Protection Regulation)
19. Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57 (Online Platforms Regulation)
20. Treaty on the Functioning of the European Union [2007] OJ C 326/01

LIST OF REGULATIONS

1. Hague Convention on Choice of Court Agreements, concluded on 30 June 2005, entered into force on 1 October 2015

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Cases C/13/702849, C/13/706680, C/13/706842 *Stichting Onderzoek Marktinformatie et al. v TikTok et al.* [2022] Amsterdam District Court
2. European Commission amicus brief, *United States v Microsoft Corporation* [2017] No. 17-2

WEBSITE REFERENCES

1. Silva de Freitas, E.; Kramer, X., *First strike in a Dutch TikTok class action on privacy violation: court accepts international jurisdiction*, 2022, [https://conflictoflaws.net/], Accessed 24 July 2023
2. Pato, A., *The EU's Upcoming Framework on Artificial Intelligence and its Impact on PIL*, 12 July 2021 [https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/], Accessed 24 July 2023
3. von Hein, J., *Forward to the Past: A Critical Note on the European Parliament's Approach to Artificial Intelligence in Private International Law*, 22 October 2020 [https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to-artificial-intelligence-in-private-international-law/], Accessed 24 July 2023
4. Institut de Droit International, *Resolution on Internet and the Infringement of Privacy: Issues of Jurisdiction, Applicable Law and Enforcement of Foreign Judgments*, 2019 (2019 IDI Resolution) [https://www.idi-iil.org/fr/publications-par-categorie/resolutions/], Accessed 24 July 2023
5. Redic, V., *The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights*, 2014, [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_175], Accessed 24 July 2023
6. FRA, *Access to data protection remedies in EU Member States*, 2013, [https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states], Accessed 24 July 2023
7. Nuyts, A., *Study on residual jurisdiction. General report*, 3 September 2007, [https://gavclaw.files.wordpress.com/2020/05/arnaud-nuyts-study_residual_jurisdiction_en.pdf], Accessed 24 July 2023

UDK 347.931:341
Original scientific paper

CROSS-BORDER SERVICE OF DOCUMENTS IN EU GOING ONLINE: IMPLEMENTATION AND IMPLICATIONS*

Martina Drventić Barišin, PhD, Postdoctoral Fellow
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
mdrventic@pravos.hr

ABSTRACT

The service of documents is crucial for the smooth initiation and operation of cross-border civil and commercial proceedings. Cross-border service of documents raises the issues on effectiveness and efficiency of proceedings together with the effective right to access a (foreign) court in terms of the language used and the effective possibility of appearing before a court. In response, international judicial cooperation in the service of documents was established and operated for decades, starting with the Hague 1965 Service Convention. The importance of proper service of documents also comes from the fact that it is a condition to recognise and enforce the final foreign judgment in different domestic, European, and international legislations. The abolition of the exequatur procedure in the context of the EU legislation in civil matters points toward an even greater need for harmonisation, which seeks to be achieved through the Service of Documents Regulation. The changes in individual lives and business operations affected by digitalisation have also led to the need for the modernisation of judicial cooperation. The Service of Document Regulation underwent the recast procedure and entered into force on 1 July 2022. It has brought novelties, given the introduction of mandatory electronic communication between the agencies and facilitating electronic and direct service. The significant changes concern the e-Codex as the mean of communication; electronic service; electronic signature of deeds, documents and forms; and assistance in address enquiries. The paper assesses the implication of using ICT in the service of documents and, at the same time, addresses whether the changes are fully up with the fast-growing general technological advancement since it seems that the implementation level still depends on the Member States.

Keywords: *Service of Documents Regulation, ICT, access to justice, e-Codex, eIDAS, e-service, address enquiries*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

The accelerated development of technology strongly affects judicial proceedings over the world. The COVID-19 pandemic has additionally encouraged the usage of electronic handling of claims, hearings, evidence taking, and delivery of justice.[1] The digitalisation-related measures evoked by the COVID-19 pandemic to overcome the limits of existing practice were expected to be temporary. Still, they had brought an increased openness towards the electronic environment and its use in court proceedings.[2] Consequently, such novelties mostly persisted even after the crisis.[3]

The usage of new technologies[4] in the field of justice comes under the title of 'electronic justice' or 'e-Justice'. Implementing e-Justice is one of the most significant challenges of the EU's national justice systems. E-Justice means the use of electronic systems to carry out activities that had been carried out so far in some other way or in a way that was much less reliant on the said systems than is envisaged for the future.[5] The use of electronic systems in judiciary affects *how* an activity or institution functions, but not what it *does*. E-Justice is ordinary justice, but making use of the tools that ICT provides in the organisation and performance of the tasks of judicial bodies.[6] The changes that e-Justice entails should, therefore, only be external and should only affect the form of the procedural acts. The use of

---

1 Onţanu, E. A., *Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure*, Oñati Socio-Legal Series, Vol. 12, No. 3, 2022, p. 585.

2 Velicogna, M., *Cross-border Civil Litigation in the EU: What Can We Learn From COVID-19 Emergency National e-Justice Experiences?*, European Quarterly of Political Attitudes and Mentalities, Vol. 10, No. 2, 2021, p. 2., Certainly, COVID-19 pandemic has only accelerated the usage of ICT in the judiciary, while it has been developing in the last decades. See, e.g.: Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, *Towards a European e-Justice Strategy*, 30 May 2008, COM(2008) 329 final; HCCH, The HCCH Service Convention in the Era of Electronic and Information Technology, 11 December 2019 The Hague (Netherlands), [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd8fe63607.pdf]; Contini, F.; Fabri, M. (eds.), *Judicial Electronic Data Interchange in Europe: Applications, Policies and Trends*, Lo Scarabeo, Bologna, 2003; Velicogna, M., *Justice systems and ICT-What can be learned from Europe*, Utrecht Law Review, Vol. 3, No. 1, 2007, pp. 29-147; Cerrillo, A.; Fabra, P. (eds.), *E-Justice: Using Information Communication Technologies in the Court System*, Information Science Reference-Imprint of: IGI Publishing, 2008.

3 Krans, B.; Nylund, A., *Civil Courts Coping with Covid-19*, in: Krans, B.; Nylund, A. (eds.), Civil Courts Coping with Covid-19, Eleven International Publishing, The Hague, 2021, p. 3.

4 Gascón Inchausti, F., *Electronic Service of Documents. National and International Aspects*, in: Kengyel, M.; Nemessányi, Z. (eds), Electronic Technology and Civil Procedure: New Paths to Justice from Around the World, Springer, Dordrecht, Heidelberg, New York, London, 2012, pp. 137-180.

5 See: Velicogna, M., *In Search of Smartness: The EU e-Justice Challenge*, Informatics, Vol. 4, No. 1, 2017, pp. 1-17.

6 Gascón Inchausti, *op. cit.*, note 4, p. 3.

electronic systems should under no circumstances jeopardise any of the safeguards applicable to judicial activities.[7]

The focal point of the EU's e-justice in civil matters is enhancing access to justice in cross-border cases. The civil procedure differs in the Member States, regardless of the specific level of harmonisation. Due to that, the litigants in Member States can face legal and practical obstacles when endeavouring to enforce their cross-border claims. Those obstacles can derive from the necessity to establish international jurisdiction properly, the need for cross-border service of documents, the taking of evidence, enforcement, diverging domestic procedures, and having to incur additional costs for local legal representation, the translation of documents, and travel expenses.[8]

All aforementioned indicates that the EU's legal framework for international judicial cooperation in civil matters needs to address the usage of technological means to improve access to justice, uphold procedural guarantees in the use of such means, secure data protection, and provide the necessary resilience of communication flows in judicial cooperation, both during usual times and in the case of lasting disruptive events.[9] As part of these efforts, the EU legislator adopted new provisions on the cross-border service of judicial and extrajudicial documents in civil and commercial matters.

Although the language of the 2007 Service of Documents Regulation[10] was drafted in a 'technology-neutral' way, modern channels of communication were not used in practice. The same can also be stated concerning the 1965 Hague Service Convention.[11] Following the recast procedure[12] the new Service of Documents

---

7 *Ibid*., p. 3.

8 Kramer, X. E., *Access to Justice and Technology: Transforming the Face of Cross-Border Civil Litigation and Adjudication in the EU*, in: Benyekhlef, K.; Bailey, J.; Burkell, J.; Gélinas, F. (eds.), eAccess to Justice, University of Ottawa Press, Ottawa, 2016, p. 354.

9 Onțanu, *op. cit.*, note 1.

10 Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulation (EC) No 1348/2000 [2007] OJ L 324, pp. 79–120 (hereinafter: 2007 Service of Documents Regulation).

11 HCCH, Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=17].

12 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) COM/2018/379 final (hereinafter: 2018 Service of Documents Regulation Proposal).

Regulation[13] has been applicable since 1 July 2022, with the exceptions of certain rules that will apply from 2025. The novelties introducing the usage of modern technologies in the service of documents will be presented below.

2. SERVICE OF DOCUMENTS AND MODERN TECHNOLOGIES

COVID-19 was not the sole factor that demanded the implementation of digitalisation in court proceedings. In the past few years, there has been an increased number of social and commercial interactions in the European Union, closely related to the greater mobility of the new generation of workers and the rise of international e-commerce. This led to an increased number of cross-border disputes, seeking a framework to remedy the challenges of an increasingly integrated mobile and digital society.[14]

The procedural system of every state opts for the rules on the service of documents which regulate how the written communication between the court and the parties is to be conducted.[15] The national legislations on the service of documents are designed for domestic cases, not the ones with the cross-border element. For that reason, cooperation between the states is necessary.

The international law of service of documents needs to reconcile the interest between the right to effective access to justice of the party interested in proper service, and the right to be heard of the recipient. The party interested in proper service, usually the plaintiff, desires speedy transmission. While the recipient, usually the defendant, has the interest in a right to a reasonable opportunity to take note of the documents as well as comprehensibility.[16] The interests of both confronting parties need to be in line with the principle of economic procedure which implies simple, cost-effective and expeditious service. Finally, this all requires the avoid-

---

13 Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (recast) [2020] OJ L 405, pp. 40–78 (hereinafter: 2020 Service of Documents Regulation).

14 See: Amato, R.; Velicogna, M., *Cross-Border Documents Service Procedures in the EU from the Perspective of Italian Practitioners – The Lesson Learnt and the Process of Digitalisation of the procedure trough e-Codex*, Laws, Vol. 11, No. 6, 2022, pp. 1-2.

15 The notion of "service of document", need to be distinct from the notion of "service of process". Service of process regulates how to give notice of the initiation of proceedings to the defendant. McClean, D., *Service of Process*, Beaumont, P.; Holliday, J. (eds), A Guide to Global Private International Law, Hart, Oxford, London, New York, New Delhi, Sydney, 2022, pp. 161-175.

16 Kieninger, E.-M.; Hau, W., *Service of documents*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensi, P. (eds.), Encyclopaedia of Private International Law, Edward Elgar Publishing, Cheltenham, UK, Northampton MA, USA, 2017, p. 1628.

ance of mistakes which could compromise the success of subsequent proceedings, namely the recognition and enforcement of the expected decision abroad.[17]

The 1965 Hague Service Convention is technology-neutral in its current form and its usefulness and applicability in the future depends on the embrace of modern technology.[18] The Conclusions and Recommendations of the Special Commission on the Practical Operation of The Hague Apostille, Evidence and Service Conventions reaching far in 2003 emphasized the need to embrace technical developments and acknowledged that modern technologies are an integral part of life today.[19] Specifically, the Special Commission recommended that States explore ways to use modern technology to further the operation of the Service Convention, especially in regard to the electronic transmission of requests.[20] The trend in advocating the digitalisation within the 1965 Hague Service Convention is continuous, this was confirmed by further discussion within the Special Commissions[21] and the 4th edition of Practical Handbook on the Operation of the Service Convention, giving the special focus to modern technologies.[22]

The 2007 Service of Documents Regulation was also drafted as an technology-neutral tool. The Commission had argued that the traditional channels of transmission of a document were underperforming and modern channels of communication are in practice not used due to old habits, legal obstacles, and lack of interoperability of the national IT systems.[23] The research on the functioning of the EU instruments regulating the cooperation in civil matters had identified the

---

17 *Ibid*.

18 Ossenova, K. V., *Use of an Electronic Platform for Communication and Transmission Between Central Authorities in the Operation of the HCCh Service Convention*, HCCH a|Bridged Edition, The HCCH Service Convention in the Era of Electronic and Information Technology, The Hague, 2019, [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd8fe63607.pdf], p. 14.; Richard, V.; Hess, B., *The 1965 Service and 1970 Evidence Conventions as crucial bridges between legal traditions?*, in: John, T.; Gulati, R.; Köhler, B. (eds.), The Elgar Companion to the Hague Conference on Private International Law, Elgar, Cheltenham and Northampton, 2020, pp. 288-298.

19 HCCH, Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Apostille, Evidence and Service Conventions, 2003, [https://assets.hcch.net/docs/0edbc4f7-675b-4b7b-8e1c-2c1998655a3e.pdf].

20 *Ibid*.

21 HCCH, Conclusions and Recommendations of the Special Commission on the practical operation of The Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions, 2009, [https://assets.hcch.net/upload/wop/jac_concl_e.pdf]; *Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Service, Evidence and Access to Justice*, 2014, [https://assets.hcch.net/docs/eb709b9a-5692-4cc8-a660-e406bc6075c2.pdf].

22 HCCH, *Practical Handbook on the Operation of the Service Convention*, 4th ed., The Hague, 2016, [https://www.hcch.net/en/publications-andstudies/details4/?pid=2728&dtid=3].

23 2018 Service of Documents Regulation Proposal, p. 3.

service of documents as a universal problem.[24] Kramer those difficulties in cross-border service of documents associates with differences between national rules on service, the plurality of authorities involved and their different work methods, language requirements and other formalities, which result in delays in the actual service to the addressee and obtaining proof thereof.[25]

The evaluations that had proceeded the Proposal for the amendment of the 2007 Service of Documents Regulation identified the shortcomings in the protection of procedural rights and overall legal complexity and uncertainty and concluded that benefits would result from using electronic communication for digitalisation of the judiciary, by simplifying and speeding up cross-border judicial procedures and judicial cooperation.[26] The intention of the legislator was to make the substantial improvement with little investment by relying on the EU outputs and legal standards that already exist.[27] The proposal was published in 2018 and offered a new set of rules aimed at improving the effectiveness and speed of judicial procedures, primarily by digitalising them. The Commission's idea was as well to rely on EU outputs and legal standard that already existed, such as e-Codex,[28] a European digital infrastructure for secure cross-border communication in the field of justice developed and managed by a consortium of Member States with EU co-funding and applied in voluntary pilot projects by a number of Member States.[29] Nevertheless, the Regulation was drafted before the COVID-19 pandemic and before the EU took a systematic approach to regulating the digitalisation of justice. Regardless, the Proposal and final text are aligned with the latest EU policies, including the EU's digitalisation of the judicial cooperation package.[30] The new 2020

---

24 Gascón Inchausti, F.; Requejo Isidro, M., *A Classic Cross-border Case: the Usual Situation in First Instance*, in: Hess, B.; Ortolani, P. (eds.), Impediments of National Procedural Law to the Free Movement of Judgments, Vol. I, Beck/Hart/Nomos, Oxford/Baden-Baden, 2019, pp. 5–85.

25 Kramer, X., *Are you Being Served? Digitising Judicial Cooperation and the HCCH Service Convention*, HCCH a|Bridged Edition, The HCCH Service Convention in the Era of Electronic and Information Technology, The Hague, 2019, [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd-8fe63607.pdf], p. 44.

26 2018 Service of Documents Regulation Proposal, p. 7.

27 *Ibid*., p. 3.

28 Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726, PE/87/2021/REV/1 [2022] OJ L 150, p. 1–19.

29 See: Francesconi, E.; Peruginelli, G.; Steigenga, E.; Tiscornia, D., *Conceptual Modeling of Judicial Procedures in the e-Codex Project*, in: Casanovas, P.; Pagallo, U.; Palmirani, M.; Sartor, G. (eds.), AI Approaches to the Complexity of Legal Systems, Vol 8929, 2014, Springer, Berlin, Heidelberg, pp. 202-216.

30 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

Service of Documents Regulation pursues two objectives. The first is to modernise the system of both exchanges between authorities and agencies and direct service to the recipient through the introduction of digital communication on a mandatory basis (between authorities) or in the case of the recipient's consent (for direct service). And second, to address the shortcomings in the previous Regulation clarity or its operation in practice.[31]

3. DIGITALISATION RELATED NOVELTIES IN 2020 SERVICE OF DOCUMENT REGULATION

3.1. Communication between Transmitting and Receiving Agencies and Central Bodies

The introduction of modern communication technologies opened the issue of communication between the authorities seated in the different states and its transformation from traditional paper communication to electronic communication. Electronic communication is not only necessary to keep up with modern society's demands but also contributes to equally efficient and secure service.[32]

The EU legislator intended to establish a system grounded on principles of speediness and efficiency,[33] which strongly relies on direct transmission of documents between the authorities, without recourse to diplomatic channels, which are foreseen only in exceptional circumstances.[34] For that reason the Service Regulation obliges the Member States to designate the transmitting agencies and receiving agencies.[35]

The 2007 Service of Documents Regulation provided that the transmission of documents between the transmitting and receiving agencies could be carried out by any appropriate means provided that the content of the document received is true and faithful to that of the document forwarded and that all information in it is easily legible. This technology-neutral formulation permitted electronic exchanges, but they were not used in practice.[36] Regulation did not set any particular

---

amending certain acts in the field of judicial cooperation, SEC(2021) 580 final,S WD(2021) 392 final, SWD(2021) 393 final.

31 Stein, A., *The European Service Regulation: Introduction*, in: Anthimos, A.; Requejo Isidro, M. (eds.), The European Service Regulation. A Commentary, Edward Elgar Publishing, Cheltenham/Northampton, 2023, pp. 1-25.

32 Kramer, *op. cit.*, note 25, p. 45.

33 Dominelli, S., *Current and Future Perspectives on Cross-Border Service of Documents*, Scritti di diritto privato europeo e internazionale, Aracne, 2018, p. 78.

34 2020 Service of Documents Regulation, Article 16.

35 *Ibid.*, Article 3.

36 Stein, *op. cit.*, note 30, p. 4.

time limit for the agency to transmit the documents to the foreign agency following the request of the interested party.

The new rules of the 2020 Service of Documents Regulation do not change the core of the provision on the transmission of documents between the agencies, it only changes the medium through which transmission must be performed.[37] The central rule establishes an obligation for all communication and exchanges of documents between the agencies and bodies designated by the Member States to be carried out by a secure and reliable decentralised IT system.[38] The Regulations mentions the e-Codex as an example of a decentralised IT system. That's because it was not the intention of the legislator to tie the Regulation to e-Codex firmly, but to leave space for more advanced technical solutions in the future.[39]

No later than 1 May 2025,[40] when the provision enters into force, all the technical measures have to be taken to make this ICT system operational, and the transmitting agencies should be able to use their usual national application interface or software provided by the European Commission to send the documents to be notified to the receiving agencies via the e-CODEX system.[41] The specific standard form of the request will be completed in electronic format in one of the official languages of the requested State or in a language accepted by that State.[42] The receiving agency, for its part, will send an automatic acknowledgement of receipt to the transmitting agency via the same system, using the electronic version of the forms.[43]

The 2020 Service of Documents Regulation also refers to the eIDAS Regulation.[44] This Regulation is generally applicable to the electronic transmission of documents and clarifies that qualified electronic seals or signatures, as defined in it, may be

37 Amato, Velicogna, *op. cit.*, note 14, p. 21.

38 2020 Service of Documents Regulation, Article 5.

39 Stein, *op. cit.*, note 30, p. 4.

40 2020 Service of Documents Regulation, Article 37; The provision on means of communication between Transmitting and Receiving Agencies and Central Bodies will come into force on 1 May 2025, three years after the entry into force of the Implementing Act establishing the decentralised IT system, which was adopted on 14 March 2022.; Commission Implementing Regulation (EU) 2022/423 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1784 of the European Parliament and of the Council, C/2022/1417 [2022] *OJ L 87, p. 9–13.*

41 Amato, Velicogna, *op. cit.*, note 14., p. 21.

42 2020 Service of Documents Regulation, Article 8(2).

43 *Ibid.*, Article 10(1).

44 *Ibid.*, Article 5(3); Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257, p. 73–114.

used where documents transmitted require or feature a seal or a handwritten signature. Following that, all documents passing between transmitting and receiving agencies will be able to be signed electronically and will not be deprived of legal effect or considered inadmissible simply because they are in electronic format.[45]

The transmission can be carried out by other mean only if there is a disruption of the decentralised IT system or due to exceptional circumstances.[46] Examples of exceptional circumstances can be found in the Recitals. They are related to situations in which the voluminous documentation in electronic form will be a large administrative burden for transmitting agency or whereby the original document is needed in paper format to assess its authenticity.[47] The question is to what extent the States will use this exception since many cases and documentation are voluminous, and there are still many decisions and documentation without electronic signature. Will those exceptions also lead to the abuse of this new provision on communication just because national authorities will still rather communicate old-fashioned way? Anyhow, these exceptions have to be interpreted narrowly due to the explicit aim of the Regulation to make the transmission via a decentralised IT system mandatory.

3.2. Cooperation in Address Enquiries

Indirectly, the digitalisation of the administrative cooperation also loosens up the scope of application of the 2020 Service of Documents Regulation. The old rules of the 2007 Service of Documents Regulation strictly excluded the application of the Regulation where the address of the person to be served with the document was not known.[48] The difficulties in application in this regard were identified.[49] There were situation is which the parties expected Central Authorities to locate the recipient or have made use of the Evidence Regulation to locate the address (even this Regulation as well preconditions the knowledge of the address for its application).[50]

---

45 2020 Service of Documents Regulation, Article 6.

46 *Ibid*., Article 5(4).

47 *Ibid*., Recital 15.

48 2007 Service of Document Regulation, Article 1(2); same as the 1965 Hague Service Convention, Article 1(2).

49 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Regulation (EC) NO 1393/2007 on the European Parliament and the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, COM/2013/0858 final, point. 3.2.1.

50 *Ibid*.; 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, p. 1–24.

The purpose of such a rule in 2007 Service of Document Regulation was to avoid imposing excessive obligations on the Member States and to avoid the question to whom the duty to find the address might fall.[51] However, the Brussels I*bis* Regulation[52] and Brussels II*ter* Regulation,[53] provided that where the defendant does not enter an appearance, the court has to stay the proceedings so long as it cannot be shown that the defendant has been able to receive the document instituting the proceedings in sufficient time to enable him to arrange for his defence, or that all necessary steps have been taken to this end.[54] The CJEU further elaborated those "necessary steps" in the meaning that the court seized of the matter must be satisfied that all investigations required by the principles of diligence and good faith have been undertaken to trace the defendant.[55]

The new rules of 2020 Service of Document Regulation opt for the same solution as its predecessor, but with the exception of Article 7.[56] Whole new Article provides for assistance in address enquiries, to some extent relying on the means of modern technologies. The provided procedures represent some specific measure or pre-step before the service occurs or after the unsuccessful service occurs. A similar system is provided and well-functioned under the Maintenance Regulation, which governs the specific measure in finding the debtor's address.[57]

In situations where the address of the person to be served with the judicial or extrajudicial document in another Member State is unknown, Member State is obliged to provide the assistance. The provision provides for three types of assistance. Member State shall assist in determining the address in at least one of these ways. First, by providing for designated authorities to which transmitting agencies may address requests to determine the address of the person to be served. The examples of such designated authorities are the same ones designated as the receiving

---

51 Dominelli, *op. cit.*, note 33., p. 71.

52 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) [2012] OJ L 351, p. 1–32, Article 28(2).

53 Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast), ST/8214/2019/INIT [2019] OJ L 178, p. 1–115, Article 19(1).

54 Stein, *op. cit.,* note 30, p. 39.

55 Case C-327/10 *Hypoteční banka a.s.* [2011] EU:C:2011:745, para. 52.; Case C-292/10 *Cornelius de Visser* [2012] EU:C:2012:142, para. 55.

56 2020 Service of Documents Regulation, Article 1(2).

57 See: Council Regulation (EC) No 4/2009 of 18 December 2008 on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations [2009] OJ L 7, p. 1–79, Article 51(2)(b) in conjunction with Article 52.; Župan, M.; Drventić, M., *Sustav središnjih tijela kroz europski model naplate prekograničnog uzdržavanja*, Zbornik radova Dani porodičnog prava „Pravna sredstva za smanjenje siromaštva djece", Mostar, 2015, pp. 151-161.

agencies (Czech Republic, Italy, Slovenia, Spain, Slovakia) or designated as central authorities (Cyprus, Hungary, Romania). Other designated authorities are bailiffs (Belgium, Latvia, Lithuania, and Luxembourg), the Ministry of Interior (Croatia), the civil registry (Estonia) or the national court registry (Poland).[58]

The second type of assistance is allowing persons from other Member States to submit requests, including electronically, for information about addresses of persons to be served directly to domicile registries or other publicly accessible databases using a standard form available on the European e-Justice Portal. None of the Member States provided for such kind of assistance. The reason for that possibly lies in the fact that it is not fully clear who is the "person from the other Member State", does this concern the official person or any interested party – physical person to use the assistance. In this regard, the Member States mostly remained in the framework of secure and official communication indicated by the transmitting agencies and thus had chosen the first mean of assistance.

The third mean of assistance relates to the detailed information provided by the Member States, through the European e-Justice Portal, on how to find the addresses of persons to be served. This model may concern as the "easiest way out" for Member States to comply with the imposed obligation.[59] It comes in the form of detailed information on national law and procedure for obtaining information from the population register (Germany, Austria), provided information on online phone registries or business registries, and other helpful information for individual research (Ireland, France), or a combined system where there is information provided on the separate registries for the natural persons, and information on the registries for companies (Latvia, Malta, Finland).[60] Overall, this model concerns the possibility to contact the particular registry online or to make an individual research on publicly available online databases.

By this provision, the legislator decided to add an option for the party interested in service to have a more significant probability for successful service when the address of the person to be served is unknown. In this case, the Regulation does not follow the well-functioned system of cooperation between the Member States from Maintenance Regulation. Although this might be a good solution,[61] in this case, it is decided not to put an excessive burden on the requested Mem-

58 E-Justice Portal, European Judicial Atlas in Civil Matters, *Serving Documents (Recast)*, [https://e-justice.europa.eu/38580/EN/serving_documents_recast], Accessed 25 June 2023.

59 Stein, *op. cit.*, note 31, p. 10.

60 E-Justice Portal, *op. cit.*, note 58.

61 Dominelli, *op. cit.*, note 32, p. 73.

ber States.[62] It is without question that these new rules will help in the search for unknown addresses. Still, this new measure is not uniform, meaning that the provided assistance models differ in effectiveness, mainly because there is a variety of authorities involved and methods of finding the address. It is questionable to what extent its purpose will be accomplished in practice.

3.3. Electronic Service

The electronic service of documents can be very useful in an international environment where borders are no barriers to electronic communication, which leads to the some advantages of procedural efficiency.[63] Necessary condition for the exercise of the right to be heard is that the party becomes aware of an act in respect of which he has a right to be heard, any caution in the regulation of the electronic service of documents in the cross-border environment is thus justified. The proper service of the documents to the defendant is the core basis for the defendant's right of defence. Unlike the traditional means of service, the electronic service does not always guarantee appropriate recognition by a defendant. For that reason, Member States usually do not accept electronic service as a primary service method without the defendant's consent. Overall, the solutions in the Member States differ, with the examples where the electronic service is already standard.[64]

Until the 2020 Service of Document Regulation, there was no reference to electronic service in international and EU instruments regulating the cross-border service of documents.[65]

---

62 It should bear in mind that the functions of Central Authorities in family matters are always more specific and justified. See: Župan, M.; Christian H.; Ulrike K., *Central Authority Cooperation Under The Brussels II ter Regulation*, in: Bonomi, A.; Romano, G. P. (eds.), Yearbook of Private International Law, Vol. XXII, 2020/2021, Verlag Dr. Otto Schmidt, Köln, 2021, pp. 183-200; Župan, M., *Cooperation between Central Authorities, Jurisdiction in Matrimonial Matters*, in: Honorati, C. (ed.), Parental Responsibility and International Abduction: A Handbook on the Application of Brussels IIa Regulation in National Courts, Peter Lang, Frankfurt am Main, 2018, pp. 265-292.

63 Gascón Inchausti, *op. cit.*, note 4, p. 173.

64 E.g. Austria, which introdouced the system *Elektronischer Rechtsverkehr* (ERV) for digital service in 1990s.

65 Although, EU legislator already introduced the electronic service within the uniform procedures regulation of the European Enforcement Order, European Order for Payment Procedure and European Small Claim Procedure. See: Regulation (EC) No 805/2004 of the European Parliament and of the Council of 21 April 2004 creating a European Enforcement Order for uncontested claims [2004] OJ L 143, p. 15, Article 13(1)(d) and 14(1)(f).; Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure [2006] OJ L 399, p. 1–32, Article 13(1)(d) and 14(1)(f); Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure [2007] OJ L 199, p. 1, Article 13(1)(b).

The 2020 Service of Regulation changes the current legal framework as it introduces electronic service of documents as an additional alternative method of service in cross-border cases.[66] The new provision on direct electronic service is less ambitious than the one proposed in 2018 but still represents a step forward to the use of electronic communication channels.[67] The provision should be interpreted as granting the choice to the court of proceedings to make use of other methods if, on a case by case approach, service by email might prejudice the right to defence, or be impossible for technical reasons.[68]

Provision provides that direct service can be effected only by electronic means that are available for domestic service under the law of the Member States.[69] This solution pre-conditions the general use of electronic service to its development in Member States where the national solution greatly differ.[70] As to the current state, 11 Member States declared that they do not apply the Article 19 on electronic service (Spain, Croatia, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Finland, and Sweden), which calls into question true technological advances in terms of service of documents.[71]

The provision provides for two alternative models of direct electronic service. They are both conditioned by the prior consent of the addressee. The first method is electronic service by using qualified electronic registered delivery services within the meaning of eIDAS Regulation, where the addressee must give prior express consent to the use of electronic means for service of documents in the course of legal proceedings. It can be assumed that this will mean that qualified electronic registered delivery services which are already operating in the Member States would be extended to the cross-border service.[72] Regarding the consent, prior express consent could be given for specific proceedings or as a general consent to the service of documents in the course of legal proceedings by those means of service. Where under the law of the forum Member State procedural documents can be served through an electronic system, it is sufficient to express prior consent to

66 2020 Service of Documents Regulation, Article 19.

67 Stein, *op. cit.*, note 30, p. 6.; The final content of the Article 19 can be considered as the result of the consensus between the Member State.

68 Dominelli, *op. cit.*, note 32, p. 154.

69 The 2018 did not included this condition in the proposed provision, see: 2018 Service of Document Regulation Proposal, Article 15. Still, this condition is of the European Order for Payment Procedure and European Small Claims Procedure, Article 13(1)(b).

70 Stein, *op. cit.*, note 30, p. 6.

71 E-Justice Portal, *op. cit.*, note 58.; It should be noted that the information provided on the e-Justice Portal are still incomplete and does not contain the data for all the Member States. Objections can also be made to the clarity and precision of the submitted answers.

72 *Ibid*.

the service of documents, where the explicit reference to court proceedings is not necessary.[73]

The second method provides the electronic service via simple email. In this case, the addressee must express its prior consent with regard to specific court proceedings. The addressee also needs to confirm the receipt, including the date of receipt.[74] The addressee should confirm receipt of the document by signing and returning an acknowledgement of receipt or by returning an email from the email address furnished by the addressee for service. The acknowledgement of receipt could also be signed electronically.[75]

The provision as well permits the Member States to predict additional requirements to guarantee the safety of the transmission.[76] Such conditions could address issues such as the identification of the sender and the recipient, the integrity of the documents sent and the protection of the transmission against outside interference.[77] Only four countries declared that they do no ask for the additional requirements (Slovenia, Austria, Hungary, and Ireland), while five of them declared on the need to meet additional condition in the application of the provision on electronic service (Belgium, Czech Republic, Estonia, France, Slovakia).

The cumulation of strict conditions for electronic service prescribed by the provision itself, the possibility of Member States to impose additional conditions themselves, together with the current data provided on the e-Justice Portal, indicate that the real benefits of electronic service at the EU level are hardly achievable at this time.

4. CONCLUSION

The development of electronic technology in our society started two decades ago. Nowadays, there are highly developed and sophisticated means of electronic communication. Due to their convenience and effectiveness, their application in civil justice procedures is inevitable and appropriate.

The 2020 Service of Documents Regulation replaces the paper-based transmission mechanism with the decentralised ICT system of national applications interconnected by a secure and reliable communication infrastructure – e-Codex. The

---

73 2020 Service of Documents Regulation, Recital 32.

74 *Ibid.*, Article 19(1)(b).

75 *Ibid.*, Recital 33.

76 *Ibid.*, Article 19(2).

77 2020 Service of Documents Regulation, Recital 33.

new framework relies on the broader and better use of technological solutions. This framework offers promising opportunities to improve the system in terms of efficiency. It reduces notification time and security problems and offers direct and secure communication channels. The overall time left for implementing those provisions in national systems is reasonable. Still, there is a certain doubt about resorting to the traditional transmission channels due to the exceptions provided in the recital.

By providing assistance in address enquiries, the legislator decided to add an option for the party interested in service to have a more significant probability for successful service when the address of the person to be served is unknown. In this case, it is decided not to burden the requested Member States excessively. Instead, the Member States can choose one or more proposed assistance models, which include different authorities and work methods. It is without question that these new rules will help in the search for unknown addresses. Still, this new measure is not uniform, meaning that the provided assistance models significantly differ in effectiveness.

The new provision on electronic service grants to the court of proceedings the choice to decide whether it will use the electronic service, if the electronic mean of service is available under its national law. By providing strict conditions to use this service method and allowing Member States to add additional requirements, the Regulation leaves a small place for the procedural safeguards to be breached. Still, those strict conditions, together with the data on national laws provided on the e-Justice Portal, indicate that the full benefits of electronic service at the EU level are hardly reachable.

The recast procedure had two objectives - to introduce digital communication and to address the existing shortcomings in previous Regulation concerning its clarity and operation in practice. Unfortunately, everything indicates that the new provisions on digitalisation are introducing new shortcomings in the sense of their clarity and implementation. The new rules are not in line with the advancement of modern technology and thus not contribute to the expected enhancement of the individual's right to access to justice.

REFERENCES

BOOKS AND ARTICLES

1. Amato, R.; Velicogna, M., *Cross-Border Documents Service Procedures in the EU from the Perspective of Italian Practitioners – The Lesson Learnt and the Process of Digitalisation of the procedure trough e-Codex*, Laws, Vol. 11, No. 6, 2022, pp. 1-28
2. Cerrillo, A.; Fabra, P. (eds.), *E-Justice: Using Information Communication Technologies in the Court System*, Information Science Reference-Imprint of: IGI Publishing, 2008
3. Contini, F.; Fabri, M. (eds.), *Judicial Electronic Data Interchange in Europe: Applications, Policies and Trends*, Lo Scarabeo, Bologna, 2003
4. Dominelli, S., *Current and Future Perspectives on Cross-Border Service of Documents*, Scritti di diritto privato europeo e internazionale, Aracne, 2018
5. Francesconi, E.; Peruginelli, G.; Steigenga, E.; Tiscornia, D., *Conceptual Modeling of Judicial Procedures in the e-Codex Project*, in: Casanovas, P.; Pagallo, U.; Palmirani, M.; Sartor, G. (eds.), AI Approaches to the Complexity of Legal Systems, Vol. 8929, Springer, Berlin, Heidelberg, 2014, pp. 202-216
6. Gascón Inchausti, F.; Requejo Isidro, M., *A Classic Cross-border Case: the Usual Situation in First Instance*, in: Hess, B.; Ortolani, P. (eds.), Impediments of National Procedural Law to the Free Movement of Judgments, Vol. 1, Beck/Hart/Nomos, Oxford/Baden-Baden, 2019, pp. 5–85
7. Gascón Inchausti, F., *Electronic Service of Documents. National and International Aspects*, in: Kengyel, M.; Nemessányi, Z. (eds.), Electronic Technology and Civil Procedure: New Paths to Justice from Around the World, Springer, Dordrecht, Heidelberg, New York, London, 2012, pp. 137-180
8. Kramer, X. E., *Access to Justice and Technology: Transforming the Face of Cross-Border Civil Litigation and Adjudication in the EU*, in: Benyekhlef, K.; Bailey, J.; Burkell, J.; Gélinas, F. (eds.), eAccess to Justice, University of Ottawa Press, Ottawa, 2016, pp. 351-377
9. Kramer, X., *Are you Being Served? Digitising Judicial Cooperation and the HCCH Service Convention*, HCCH a|Bridged Edition, The HCCH Service Convention in the Era of Electronic and Information Technology, The Hague, 2019, [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd8fe63607.pdf], pp. 44-47
10. Kieninger, E.-M.; Hau, W., *Service of documents*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensi, P. (eds.), Encyclopaedia of Private International Law, Edward Elgar Publishing, Cheltenham, UK, Northampton MA, USA, 2017, pp. 1628-1634
11. Krans, B.; Nylund, A., *Civil Courts Coping with Covid-19*, in: Krans, B.; Nylund, A. (eds.), Civil Courts Coping with Covid-19, Eleven International Publishing, The Hague, 2021, pp. 1-7
12. McClean, D., *Service of Process*, in: Beaumont, P.; Holliday, J. (eds.), A Guide to Global Private International Law, Hart, Oxford, London, New York, New Delhi, Sydney, 2022, pp. 161-175
13. Onţanu, E. A., *Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure*, Oñati Socio-Legal Series, Vol. 12, No. 3, 2022, pp. 582–613

14. Ossenova, K. V., *Use of an Electronic Platform for Communication and Transmission Between Central Authorities in the Operation of the HCCh Service Convention*, HCCH a|Bridged Edition, The HCCH Service Convention in the Era of Electronic and Information Technology, The Hague, 2019, [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd8fe63607.pdf], pp. 14-20
15. Stein, A., *The European Service Regulation: Introduction*, in: Anthimos, A.; Requejo Isidro, M., The European Service Regulation. A Commentary, Edward Elgar Publishing, Cheltenham, Northampton, 2023, pp. 1-25
16. Velicogna, M., *Cross-border Civil Litigation in the EU: What Can We Learn From COVID-19 Emergency National e-Justice Experiences?*, European Quarterly of Political Attitudes and Mentalities, Vol. 10, No. 2, 2021, pp. 1-25
17. Velicogna, M., *In Search of Smartness: The EU e-Justice Challenge*, Informatics, Vol. 4, No. 1, 2017, pp. 1-17
18. Velicogna, M., *Justice systems and ICT-What can be learned from Europe*, Utrecht Law Review, Vol. 3, No. 1, 2007, pp. 29-147
19. Župan, M.; Christian H.; Ulrike K., *Central Authority Cooperation Under The Brussels II ter Regulation*, in: Bonomi, A.; Romano, G. P. (eds.), Yearbook of Private International Law, Vol. XXII, 2020/2021, Verlag Dr. Otto Schmidt, Köln, 2021, pp. 183-200
20. Župan, M., *Cooperation between Central Authorities, Jurisdiction in Matrimonial Matters*, in: Honorati, C. (ed.), Parental Responsibility and International Abduction: A Handbook on the Application of Brussels IIa Regulation in National Courts, Peter Lang, Frankfurt am Main, 2018, pp. 265-292
21. Župan, M.; Drventić, M., *Sustav središnjih tijela kroz europski model naplate prekograničnog uzdržavanja*, Zbornik radova Dani porodičnog prava „Pravna sredstva za smanjenje siromaštva djece", Mostar, 2015, pp. 151-161

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-327/10 Hypoteční banka a.s. [2011] EU:C:2011:745
2. Case C-292/10 Cornelius de Visser [2012] EU:C:2012:142

EU LAW AND OTHER DOCUMENTS

1. Commission Implementing Regulation (EU) 2022/423 of 14 March 2022 laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1784 of the European Parliament and of the Council, C/2022/1417 [2022] *OJ L 87*
2. Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, *Towards a European e-Justice Strategy*, 30 May 2008, COM(2008) 329 final
3. 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

4. Council Regulation (EC) No 4/2009 of 18 December 2008 on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations [2009] OJ L 7
5. Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast), ST/8214/2019/INIT [2019] OJ L 178
6. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) COM/2018/379 final
7. 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, SEC(2021) 580 final,S WD(2021) 392 final, SWD(2021) 393 final
8. Regulation (EC) No 805/2004 of the European Parliament and of the Council of 21 April 2004 creating a European Enforcement Order for uncontested claims [2004] OJ L 143
9. Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure [2006] OJ L 399
10. Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure [2007] OJ L 199
11. Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulation (EC) No 1348/2000 [2007] OJ L 324
12. 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) [2012] OJ L 351
13. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257
14. Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (recast) [2020] OJ L 405
15. Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726, PE/87/2021/REV/1 [2022] OJ L 150
16. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Regulation (EC) NO 1393/2007 on the European Parliament and the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, COM/2013/0858 final

HCCH CONVENTIONS AND OTHER DOCUMENTS

1. Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Apostille, Evidence and Service Conventions", 2003, [https://assets.hcch.net/docs/0edbc4f7-675b-4b7b-8e1c-2c1998655a3e.pdf]
2. Conclusions and Recommendations of the Special Commission on the practical operation of The Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions", 2009, [https://assets.hcch.net/upload/wop/jac_concl_e.pdf]
3. Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Service, Evidence and Access to Justice, 2014, [https://assets.hcch.net/docs/eb709b9a-5692-4cc8-a660-e406bc6075c2.pdf.]
4. Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, [https://www.hcch.net/en/instruments/conventions/full-text/?cid=17]
5. HCCH, *Practical Handbook on the Operation of the Service Convention*, 4th ed., The Hague, 2016, [https://www.hcch.net/en/publications-andstudies/details4/?pid=2728&dtid=3]
6. The HCCH Service Convention in the Era of Electronic and Information Technology, 11 December 2019, The Hague (Netherlands), [https://assets.hcch.net/docs/24788478-fa78-426e-a004-0bbd8fe63607.pdf]

WEBSITE REFERENCES

1. E-Justice Portal, European Judicial Atlas in Civil Matters, *Serving Documents (Recast)*, [https://e-justice.europa.eu/38580/EN/serving_documents_recast], Accessed 25 June 2023

UDK 341.3:343.222]:004
Original scientific paper

INDIVIDUAL CRIMINAL RESPONSIBILITY OF NON-STATE ACTORS OPERATING IN CYBERSPACE FOR WAR CRIMES UNDER THE ICC STATUTE*

Giulia Gabrielli, PhD, Post-doctoral Research Fellow
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
giulia.gabrielli@unimi.it

ABSTRACT

Contemporary armed conflict has witnessed an increased employment of digital technologies in the conduct of hostilities. While there is broad consensus on the full applicability of the rules and principles of international humanitarian law (IHL) to the "fifth domain" of warfare, many issues remain debated. More specifically, digital technologies allow a wide range of actors other than States – such as individuals, "hacktivists", criminal groups, non-State armed groups – to play a role in the hostilities and engage in cyber operations that have the potential of harming civilians or damaging civilian infrastructure and that may amount to serious violations of IHL.

Against this backdrop, this paper seeks to examine the legal grounds upon which hostile cyber operations carried out by non-State actors (NSAs) could constitute war crimes, thus entailing their individual criminal responsibility under international law. Hence, the analysis will focus on the applicability of the war crimes provisions of the Rome Statute of the International Criminal Court (ICC) to such operations, with a view to identifying the prerequisites necessary to trigger the ICC's jurisdiction.

To this end, the first part will focus on the increased involvement of NSAs in the conduct of hostilities by cyber means, taking the recent conflict between Russia and Ukraine as a pertinent case study. Subsequently, the paper will explore the conditions necessary for the application of Article 8 of the ICC Statute, with special attention devoted to those aspects that are deemed particularly problematic in light of the participation of NSAs in armed conflict. Finally, the paper seeks to highlight the limits of possible future investigations of cyber conducts possibly amounting to war crimes. These encompass not only issues of admissibility, but also the statu-

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

tory limits of the Rome Statute when it comes to war crimes provisions applicable to non-international armed conflicts.

***Keywords**: cyberwarfare, International Criminal Court (ICC), individual criminal responsibility, international humanitarian law, non-State actors, war crimes*

1. INTRODUCTION

In the last decades, the role of information and information technology (IT) has significantly expanded to pervade all aspects of human interaction. A variety of entities, including States and individuals, consistently rely on communication technologies to perform several functions, which range from business operations to food, water, or energy distribution, as well as transportation, finance, health care and manufacturing.

Against this backdrop, armed conflict is not exempt from the ubiquity of new technologies. Computers, computer systems and networks are increasingly used by military forces, both in their ordinary organizational activities and logistics, but also, and more notably, in the conduct of hostilities.[1] The use of means and methods of warfare that take advantage of digital technologies such as autonomous weapons systems, artificial intelligence, precision-guided munitions, etc. allow belligerents to direct their attacks with more precision, to better coordinate the action of military forces on the field, and to make informed decisions in targeting. These hence might have a positive impact on the protection of civilians during armed conflict since they might allow belligerent parties to minimize collateral damage and to reduce the need to resort to armed force to achieve certain military goals.[2]

The impact of new technologies on warfare is not strictly limited to the conduct of hostilities *per se* but extends to the investigation of human rights violations as well, by contributing to the creation of open-source repositories of digital evidence that are captured, for instance, by the mobile phones of eyewitnesses, victims and perpetrators and posted on social media. The use of digitally derived evidence[3] in criminal proceedings necessarily involves potential risks but might also be usefully

---

1 Lin, H., *Cyber conflict and international humanitarian law*, International Review of the Red Cross, Vol. 94, No. 886, 2012, p. 516.

2 *Ibidem*; International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts - Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, 22 November 2019, Report, p. 26.

3 For a debate on the challenges and opportunities of the use of digital and open-source evidence, see *To What Extent Can Cyber Evidence Repositories, and Digital and Open-Source Evidence, Facilitate the Work of the OTP, and the ICC More Generally?*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence], Accessed 15 November 2022.

integrated into international criminal investigations and prosecutions and represent new opportunities for justice.[4]

Without prejudice to the unprecedent advantages offered by IT in the framework of armed conflict and in the legal and accountability processes, new cyber technologies also present many risks and potential threats, in particular when used maliciously. Their affordability and relative accessibility allow a wide range of actors other than States, such as individual hackers, criminal groups, non-State armed groups and other non-State actors, to play a role in the hostilities and to cause considerable damage to the other actors involved, including militarily superior and better equipped States.[5] In this context, the increased involvement of non-State actors in armed conflict necessarily poses the issue of their increased capacity to engage in cyber operations that might result in harming civilians or causing damage to civilian infrastructure with potentially disastrous consequences. Although it does not seem that their involvement in the hostilities has given origin to serious humanitarian consequences to date, the development of increasingly sophisticated capabilities in cyberwarfare could potentially cause serious consequences for civilians and civilian infrastructure that might amount to serious violations of International Humanitarian Law (IHL), hence giving rise to the individual criminal responsibility of the perpetrator(s).

The International Committee of the Red Cross (ICRC) has consistently emphasized its humanitarian concern in respect to cyberwarfare,[6] which – due to its nature – has the potential of severely affecting civilians and civilian infrastructure for several reasons. Firstly, due to the increased reliance of civilian infrastructure on computer systems, cyber attacks may have a significant impact on the health-care sector and hospital systems, as well as critical installations, including the electrical networks, dams, nuclear plants, banking systems, railroads and air traffic. Secondly, due to the growing digitization, military and civilian networks are increasingly

---

4 Since 2015, the Office of the Prosecutor (OTP) of the International Criminal Court has relied on digital open-source content in the investigation of a number of cases, including satellite imaging collected by Google Earth in *Banda Jerbo*, *Abu Garda* and *Al Mahdi*, video materials and posts on social media in *Al-Werfalli* and evidence of wire transfer and pictures from Facebook in *Bemba et al.* See, in general, Costello, R. Á., *Facilitating the Use of Open Source Evidence at the International Criminal Court: Authentication and the Problem of Deepfakes*, ICC Forum, 2020 [https://iccforum.com/cyber-evidence#-Costello], Accessed 15 November 2022.

5 Roscini, M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, pp. 1-2. See also Missiroli, A., *Present Tense: Cyber Defence Matters*, in: Pawlak, P; Delerue, F. (eds.), A Language of Power? Cyber Defence in the European Union, Chaillot Paper/176, November 2022, p. 14, arguing that "digital technologies have dramatically lowered the entry barriers for new threat actors" through the so-called 'democratisation' effect.

6 Gisel L.; Olejnik, L. (eds.), *The potential human cost of cyber operations*, International Committee of the Red Cross, 2018, Report.

interconnected. On the one side, most civilian cyber infrastructure, or civilian infrastructure that relies on cyberspace, e.g. undersea fibre-optic cables, satellites, routers or nodes, may also be used by military networks and serve military purposes. Conversely, civilian air traffic control, vehicles and shipping are provided with navigation systems relying on global navigation satellite system (GNSS) satellites (e.g. BeiDou, GLONASS, GPS and Galileo), which may simultaneously be used by the military.

The implications of this growing interconnectivity are twofold. First, although there exist networks that are specifically designed for the exclusive use of the military, it is almost impossible in most cases to distinguish between cyber infrastructures that serve purely civilian and purely military purposes. Second, the interconnectivity and the 'dual use' of cyber infrastructures implies that cyber attacks directed against military targets may have effects that cannot be confined. This is the case of malwares, including viruses or worms, which – if uncontrollable – may spread indiscriminately among several systems and networks, regardless of their civilian or military nature, with possible repercussions on essential civilian infrastructure.[7]

Against the risks posed by cyber operations during armed conflict, this paper seeks to examine the legal grounds under which a hostile operation led by non-State actors could entail their international criminal responsibility under International Criminal Law (ICL). Namely, the analysis will focus on the possible application of the Rome Statute of the International Criminal Law (ICC) to such operations, with a view to examining the conditions necessary to trigger the Court's jurisdiction with respect to the provisions relating to war crimes. The paper is structured as follows: the first part will deal with the increased involvement of non-State actors in armed conflict by cyber means, by examining by way of example the recent conflict between Russia and Ukraine. Secondly, after some preliminary remarks on the scope of the present research, the attention will be drawn on the conditions of application of the Rome Statute, especially those which are deemed particularly problematic in light of the participation of NSA in armed conflict by cyber means and the issues that may arise.

---

7 See, Gisel, L.; Rodenhäuser, T.; Dörmann, K., *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, International Review of the Red Cross, Vol. 102, No. 913, 2020, p. 320; Droege, C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,* International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 538-539.

2. THE INVOLVEMENT OF NON-STATE ACTORS IN THE CONDUCT OF HOSTILITIES BY CYBER MEANS

On 26 February 2022, in response to Russian invasion of Ukrainian territory that had begun on the 24th, Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, announced with a tweet the creation of an "IT army", and called for the participation of cyber specialists from all over the world to join the "fight on the cyber front" against Russia. Thousands of people reportedly responded to the call from the Ukrainian government, which asked for the assistance of IT professionals and hackers to help defending Ukraine's infrastructure from Russian cyber-attacks, and to conduct hostile offensive cyber operations against Russia.[8] With the aim of coordinating the "IT Army", the Ukrainian government created a Telegram channel to instruct its almost 200,000 followers to use cyber and DDoS (Distributed Denial of Service)[9] attacks against a list of websites of Russian or Russian-affiliated targets, including for instance Russian banks and corporations such as Gazprom, but also government agencies, storage devices, and support for critical infrastructure.[10]

Aside from the "IT Army", other Ukrainian hacking collectives, which included for instance hackers from Ukrainian cybersecurity companies and firms, organized in self-managed cyber teams, coordinating their efforts autonomously on private-messaging channels.[11] Their cyber activities, endorsed – and to an extent even coordinated – by the government, reportedly aimed at carrying out a number

---

8 Holland, S.; Pearson, J., *US, UK: Russia responsible for cyberattack against Ukrainian banks*, Reuters, 2022 [https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/], Accessed November 2022; Schectman, J.; Bing, C., *Ukraine calls on hacker underground to defend against Russia*, Reuters, 2022, [https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/], Accessed November 2022.

9 Distributed Denial of Service (DDoS) is a technique that employs multiple computing devices (e.g., computers or smartphones), such as the bots of a 'botnet' (a network of compromised computers remotely controlled by an intruder used to conduct coordinated cyber operations), to render a certain computer system or computer systems unavailable to their users. *See* Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, Glossary definitions, p. 563 *et seq*. The Tallinn Manual 2.0 is a non-legally binding scholarly work crafted by an International Group of Experts and is considered one of the most authoritative resources regarding the applicability of international law in the cyber context. This contribution draws extensively from the legal position of the Experts in the Tallinn Manual, although occasionally diverging from their views.

10 Goodin, D., After *Ukraine recruits an "IT Army," dozens of Russian sites go dark*, Arstechnica, 2022, [https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/] Accessed November 2022.

11 Cerulus, L., *Kyiv's hackers seize their wartime moment*, Politico, 2022 [https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/], Accessed November 2022.

of offensive cyber operations, ranging from attacks against Russian websites and mobile applications to make them unavailable, to the disruption of Russian war propaganda. Moreover, these hackers reportedly engaged in identifying vulnerabilities in the Russian service systems, e.g., telecommunication, banking, energy firms, transportation and logistics services, with the purpose of transmitting the information to the Ukraine's cyber forces for the execution of their attacks.[12]

The efforts in responding to Russian invasion through cyber means was also undertaken by a number of cyber collectives composed of like-minded individuals who spontaneously decided to engage in the conflict through cyber means. These activist groups of hackers, known as "hacktivists", were increasingly involved in the Ukrainian-Russian conflict,[13] at least in its earliest phases. Among them, the notorious collective Anonymous publicly declared "cyber war against the Russian government"[14] and contextually started claiming responsibility for a series of hostile cyber incidents, including DDoS attacks, targeting governmental websites and databases, with subsequent shutdowns and malfunctions as well as leak of sensitive data and documents. Soon afterwards, other groups of hacktivists such as "Squad303"[15] and "NB65",[16] reportedly affiliated with Anonymous, claimed responsibility for the breach of several databases and data leakage.

Aside from IT specialists' and hackers' engagement in armed conflict, new technologies also allowed civilians who do not have particular expertise to become involved in the hostilities, for instance by downloading mobile apps that allow them to report the location of incoming missiles and other enemy air threats to Ukrainian forces.[17]

---

12 *Ibid.*

13 Koloßa, S., *The Dangers of Hacktivism How Cyber Operations by Private Individuals May Amount to Warfare*, 2022, [https://voelkerrechtsblog.org/the-dangers-of-hacktivism/], Accessed 4 February 2023.

14 Milmo, D., *Anonymous: the hacker collective that has declared cyberwar on Russia*, The Guardian, 2022 [https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia], Accessed November 2022.

15 *Who is Squad303 that is attacking Russia with Text Messages*, The Tech Outlook, 2022, [https://www.thetechoutlook.com/news/new-release/software-apps/who-is-squad303-that-is-attacking-russia-with-text-messages/] Accessed November 2022.

16 Johnson, B., *Hackers Turn Conti Ransomware Against Russia as Twitter Suspends Some Anonymous Accounts*, HomelandSecurity Today, 2022, [https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-turn-conti-ransomware-against-russia-as-twitter-suspends-some-anonymous-accounts/] Accessed November 2022.

17 The data collected and reported through the app, called "ePPO", reportedly allowed Ukrainian forces to shoot down a Russian cruise missile targeting critical infrastructure. It must be here noticed that mobile applications as a defensive tool have also been used in other situations. This is the case of "Sentry", used to warn civilians of imminent indiscriminate Syrian and Russian air strikes in Syria. *See* Schmitt, M. N.; Biggerstaff, W. C., *Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Par-*

In the broader picture, the involvement of entities other than States in the conduct of contemporary hostilities by cyber means is not a new phenomenon. New information technologies indeed have led to a democratization effect[18] that has allowed a variety of non-State actors (NSA), including armed groups, informal collectives of "hacktivists", and lone individuals, to conduct offensive cyber operations, including *inter alia* cyber-attacks and cyber exploitation,[19] with relative ease. Their structure, size, and internal organization vary significantly and so does their motivation: they may act for pure financial gain, as well as for personal, religious or political reasons.[20] As things stand as present, it appears that – among NSAs – cyber operations are most frequently conducted by criminal organizations mainly for economic purposes. Conversely, terrorist groups and militias seem to have limited their use of cyberspace to primarily operational purposes, recruitment, and funding.[21] The legal classification of online collectives and group of hackers has been the object of thorough discussions, in particular with regards to their qualification under IHL and the legal consequences that such qualification might entail.[22]

---

ticipating In Hostilities?, 2022, [https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/] Accessed 20 February 2023; Schmitt, M. N., *Ukraine Symposium – Using Cellphones To Gather and Transmit Military Information, A Postscript*, 2022, [https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/] Accessed 20 February 2023.

18 Missiroli, *op. cit.*, note 5.

19 "Cyber exploitation" refers to a variety of actions that are aimed at penetrating computer systems or networks used by an adversary with the purpose of obtaining information that would otherwise not be disclosed. Lin, *op. cit.*, note 1, p. 519.

20 Non-state actors may be informally classified according to their size, structure and motivation. Individual hackers might be formally or informally employed in States' armed forces units, or hired by States to conduct specific operations, or act alone. Criminal organizations may be driven to launch cyber-operations by financial interests and be involved in illegal activities related to cybercrimes. Cyber "mercenaries", whose definition does not correspond to the notion of mercenaries under IHL, are highly skilled hackers who might be hired by the public or private sector to conduct specific cyber-attacks, and are driven solely by financial motivations. Hacktivists are individuals and online collectives who are driven by political or ideological motives and are normally characterized by a loose structure. See, more specifically, Bussolati, N., *The Rise of Non-State Actors in Cyberwarfare*, in Ohlin, J., D.; Govern, K.; Finklestein, C. (eds.), *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press, Oxford, 2015, pp. 106-111.

21 Missiroli, *op. cit.*, note 5, pp. 17-18.

22 See, for instance, Buchan, R., *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, Chinese Journal of International Law, 2016, Vol. 15, No. 4, pp. 741-772; Stiano, A., *L'intervento di Anonymous nel conflitto tra Russia e Ucraina: Alcune riflessioni sullo status giuridico degli* hacker *attraverso il prisma del diritto internazionale umanitario*, Ordine internazionale e diritti umani, No. 4, 2022, pp. 982-1000.

For the purposes of our analysis, however, the attention will be limited to those cyber operations conducted by NSAs in the framework of armed conflict, which may entail the individual criminal responsibility under international law, thus excluding the cyber activities that do take place outside of such context, for instance those taking place in peacetime, and those occurring during hostilities, but which do not have a nexus with them (e.g. if motivated solely by profit).[23] Whereas cyber operations are broadly defined as "[t]he employment of cyber capabilities to achieve objectives in or through cyberspace"[24], when they are employed by military entities or to achieve military goals, they may amount to military cyber operations, or "cyber warfare".[25] As will be more accurately discussed below, although cyber operations may be conducted during peacetime or during hostilities, IHL is only applicable to cyber operations that are related to an international or non-international armed conflict.[26]

3. APPLICABILITY OF ICC'S WAR CRIMES PROVISIONS TO CYBER OPERATIONS: CONDITIONS AND LIMITS

Under Article 8 of the Rome Statute, the ICC has jurisdiction with respect to war crimes, when committed in the context of both international armed conflicts (IACs) and non-international armed conflicts (NIACs).[27] In order for a cyber conduct to amount to a war crime falling within the jurisdiction of the ICC, a few conditions are required. In the first place, such conduct must be committed during an armed conflict, whether international or non-international in character, and shall have a nexus to it. Secondly, the cyber conduct must be committed either in the territory of or by a national of a State that is party to the ICC or that has

---

23 According to Lin, the majority of offensive cyber operations up to now have been allegedly conducted by sub-national parties for financial reasons, especially those concerning cyber exploitation. When discussing the activities unrelated to an ongoing armed conflict that would not be governed by IHL, the Experts in the Tallinn Manual offer the example of a private corporation engaged in the theft of intellectual property over a competitor in the enemy State in order to achieve a market advantage. Lin, *op. cit.*, note 1, pp. 519-520; Schmitt, *op.cit.*, note 9, p. 377.

24 Schmitt, *op.cit.*, note 9, Glossary definition, p. 564.

25 Ducheine, P. A. L.; Pijpers, B. M. J., *The notion of cyber operations*, in Tsagourias N.; Buchan, R., (eds.) Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2021, pp. 290-291; Ambos, K., *Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Ambos] Accessed 20 February 2023.

26 Rule 80 of the Tallinn Manual 2.0 states that "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict." Schmitt, *op. cit.*, note 9, p. 375.

27 UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998 (Rome Statute), Article 8(1).

accepted its jurisdiction. Thirdly, it must involve the material and mental elements of the crimes under the Rome Statute and must be sufficiently grave in nature.[28]

The paragraphs below will attempt to consider some of these conditions in light of the peculiar issues and problems posed by the case under examination, that is the participation of NSA in hostilities by cyber means, and to discuss their possible persecution for war crimes under the Rome Statute.

3.1. The cyber operation must be carried out "in the context of and in association with the armed conflict"

The first pre-requisite for IHL to apply, and for a war crime to be committed, is the existence of a situation of armed conflict. Indeed, for a possible prosecution of a cyber operation as a war crime in accordance with Article 8 of the Rome Statute, it must be established beyond reasonable doubt that said cyber operation was conducted in the context of or in association with an international (IAC) or non-international armed conflict (NIAC).[29]

Neither IHL nor the Rome Statute provide for a definition of 'armed conflict'. Traditionally, reference is made to the jurisprudence of the International Criminal Tribunal for the Former Yugoslavia (ICTY), whose Appeals Chamber (AC) held in *Tadić* that an IAC exists "whenever there is a resort to armed force between States", whereas a NIAC occurs in case of "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".[30] IHL hence applies from the initiation of the hostilities and ceases to apply at the cessation of active hostilities or at the general close of military

---

[28] It must be noted that Article 8 of the Rome Statute states that the Court shall have jurisdiction over war crimes, "in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes". The plan, policy, or the large-scale commission of crimes is not a stringent prerequisite, but it falls within the discretionary power of the Court to also consider crimes that are not committed as part of a plan, policy, or large-scale commission. Rome Statute, Article 8 para. 1; Cottier, M., *Article 8, Part I: Introduction/General Remarks*, in Triffterer, O.; Ambos, K. (eds.), *The Rome Statute of the International Criminal Court: A Commentary*, 3rd edition., C.H. Beck, Hart, Nomos, 2016, p. 322; ICC, *Situation in the Islamic Republic of Afghanistan*, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan, ICC-02/17, Pre-Trial Chamber II, 12 April 2019, para. 65 (excluding that the existence of a plan, policy or large-scale commission pursuant to Article 8(1) is a condition for the ICC to exercise its jurisdiction).

[29] See, e.g. International Criminal Court (ICC), Elements of Crimes, 2011 ("Elements of Crimes"), Article 8(2)(a)(i)(4) (international armed conflicts include situations of military occupation); Article 8 (2)(c)(i)-1(4).

[30] ICTY, *Prosecutor v. Dusko Tadić*, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995, para. 70.

operations.[31] This definition has been endorsed by subsequent jurisprudence and international bodies,[32] including the ICC.[33]

In accordance with the definition provided, it is hence necessary to prove not only that an armed conflict existed at the time of the offence, but that the criminal conduct in question had a nexus with the hostilities. The question on whether IHL applies to cyber operations has been the object of intense debate, and at least three situations have been described: when the attack by cyber means is employed as part of an ongoing armed conflict; when it is conducted independently from other attacks; and when it is carried out extensively in conjunction with the use of conventional weapons, but the latter are on their own insufficient to qualify as an armed conflict.[34]

It is quite undisputed that IHL fully applies to cyber operations employed as 'force multipliers'[35] during existing conventional armed conflicts, i.e. when conducted in parallel or in addition to kinetic attacks directed against the adversary.[36] In such a case, however, in order to give rise to the applicability of IHL and consequently ensure the ICC jurisdiction, a nexus between the alleged offence perpetrated by cyber means and the armed conflict must be established. Article 8 of the Rome Statute indeed requires that the conduct be committed in the context of or in association with an already existing armed conflict.

Drawing from the ICTY's jurisprudence, it is necessary to prove that the offence is closely related to hostilities, in the sense that the armed conflict has played a prominent role in the perpetrator's ability and/or decision to commit such of-

---

31 The same set of rules also apply to situations of partial and total occupation, even if it is met with no armed resistance. See, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S. 31, Art. 2; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S. 85, Art. 2; Geneva Convention Relative to the Treatment of Prisoners of War Aug. 12, 1949, 75 U.N.T.S. 135, Art. 2; Geneva Convention Relative to the Protection of Civilian Persons in Times of War, Aug. 12, 1949, 75 U.N.T.S. 287, Art. 2(2).

32 Sassòli, M.; Bouvier A.; Quintin A., *How Does Law Protect in Law, Cases; Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, in Outline of International Humanitarian Law (3rd ed.) International Committee of the Red Cross, 2012, p. 22.

33 *Prosecutor v. Lubanga*, ICC-01/04-01/06, Trial Chamber, Judgment, 14 March 2012, para. 533.

34 Dinniss, H., *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012, pp. 127-131.

35 Roscini, M., *Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Roscini].

36 A well-known example is that of cyber operations conducted by alleged Russian hackers and targeting Georgian governmental and media websites in the framework of the 2008 international armed conflict between the Russian Federation and Georgia, which were unarguably subject to IHL applicable to IACs. Schmitt, M., *Cyber Operations and the Jus in Bello: Key Issues*, International Law Studies, Vol. 87, 2011, pp. 102-103. See, also: *ibidem*; Droege, *op. cit*, note 7, p. 542.

fence, in the way it was committed or the purposes for which it was committed.[37] The so-called *nexus requirement* has not been the object of extensive debate, as other issues have, especially considering the conventional international conflicts between States, where the actors participating in the hostilities were quite clearly defined. Conversely, as argued by Cottier, in contemporary NIACs, mixed or 'internalized' internal armed conflicts, "with often a wider array of different actors and less clear-cut front lines, the existence of a nexus frequently is less obvious".[38] Any prosecution of possible war crimes conducted by NSAs, who often operate transnationally, would therefore need to prove that the cyber operation had a link with the ongoing armed conflict. An indication of said link might be established by the fact that the victims belong to the adversary party, or that the action is undertaken in furtherance of the objectives of one party to the hostilities.[39] It must be noted that the assessment of the existence of a nexus with the armed conflict does not necessarily require a strict territorial link, provided that the nexus is otherwise established.[40]

The second hypothesis advanced acknowledges that not all cyber operations are performed in the framework of or in association with existing kinetic hostilities, but they may (and more often) consist in isolated computer network attacks carried out by States or NSAs[41] with (or without) repercussions in the kinetic world. In particular, it has been widely discussed whether cyber operations could amount to an armed conflict, and therefore trigger the applicability of IHL. In the scenario

---

37 The ICTY Trial Chamber held that, in determining whether an act is "sufficiently related to the armed conflict", the following factors can be taken into account: "the fact that the perpetrator is a combatant; the fact that the victim is a non-combatant; the fact that the victim is a member of the opposing party; the fact that the act may be said to serve the ultimate goal of a military campaign; and the fact that the crime is committed as part of or in the context of the perpetrator's official duties". Furtherly, the existence of an armed conflict need not be causal to the commission of the underlying crime, but it is required that such crime was committed because of the existence of a situation of armed conflict. ICTY, *Prosecutor v. Kunarac et al.,* IT-96-23 & IT-96-23/1-A, Appeals Chamber Judgment, 12 June 2002, paras. 58-60.

38 Cottier, *op. cit.*, note 28, p. 314 fn 56.

39 *See*, Schmitt, *op.cit.*, note 9, p. 392 (Rule 84 establishing the individual criminal responsibility for war crimes "does not apply to individuals engaged in purely criminal cyber operations or malicious cyber activities unrelated to the on-going international or non-international armed conflict").

40 One example is represented by the decision of the Appeals Chamber in the situation in the Islamic Republic of Afghanistan, which authorized an investigation on alleged war crimes and crimes against humanity related to the situation even when the alleged conduct occurred outside Afghan territory, and when the victims were captured outside of Afghanistan. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17-138 OA4, Appeals Chamber, Judgment, 5 March 2020.

41 A famous example of an isolated computer network attack is the Stuxnet virus, introduced into the computers of two uranium facilities in the Islamic Republic of Iran at Natanz between 2009 and 2010. Droege, *op. cit.*, note 7, p. 542.

under consideration, our analysis being focused on the cyber activity of NSAs that may have the potential to negatively affect civilians or civilian infrastructure, it is worth considering whether and under which conditions such operations conducted outside the framework of armed conflict may autonomously amount to a NIAC. In determining whether cyber operations conducted in absence of kinetic armed conflict could amount to a NIAC, two criteria shall be considered: intensity and organization.[42]

Paragraphs (c)(d) and (e)(f) of Article 8 of the Rome Statute apply to NIACs and respectively cover serious violations of article 3 common to the four Geneva Conventions of 1949, when committed against persons who do not take active part in the hostilities, and other serious violations of the laws and customs applicable to conflicts not of an international character. The minimum level of intensity that the hostilities shall reach for IHL to apply slightly differ under the two sets of provisions of the Rome Statute covering NIACs.[43]

The minimum threshold required under Article 8 para. 2 (c) and (d) is the lowest one and is negatively defined by common article 3[44] excluding from the definition of NIACs "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature".[45] This threshold hence typically requires some sort of continuity in the armed confron-

---

42 *Tadić*, *op. cit.*, note 30, para. 572.

43 It must be noted that under contemporary IHL at least three different regimes of 'minimum thresholds' can be distinguished: NIACs under common article 3, NIACs under Article 8(2)(e) and (f) of the Rome Statute of the ICC, and NIACs under Article 1 of Additional Protocol II, which is the highest threshold required and will not be addressed here. See, more accurately, Cottier, *op. cit.*, note 28, pp. 312-314.

44 In Article 8(2)(c) a certain number of guarantees for the "persons who do not take active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention or any other cause" are set forth, and they include *inter alia* the prohibition of violence to life and person, the outrages against personal dignity, the taking of hostages, and the passing of sentences or carrying out of execution without appropriate judicial safeguards. Its application is regulated by subsequent paragraph (d), which states that paragraph (c) "applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature". Rome Statute, Article 8(2)(c) and (d).

45 *Ibidem*, citing: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) of 8 June 1977 (AP II), Article 1 para. 2. State practice has confirmed that the qualification of non-international armed conflicts as excluding situations of internal disturbances, riots, isolated and sporadic acts, and other acts of similar nature as provided in AP II is applicable to common Article 3 as well. See in this respect: ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949, Commentary of 01.01.2020, Article 3 - Conflicts not of an international character, [https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020] Accessed 27 February 2023, paras. 420, 465.

tation between armed forces of a State and non-State armed groups, or among these groups.[46] In addition to the level of the armed violence, which shall not be sporadic, the armed groups involved must meet a certain degree of organization in order for the armed conflict threshold to be satisfied and IHL to be applicable, as is suggested by State practice and *opinio iuris*.[47]

The other threshold provided by Article 8 para. 2 (e) and (f) does not essentially differ from the threshold of common article 3. However, by reproducing the definition adopted by the AC in *Tadić*, these paragraphs are applicable when there is a *protracted* armed conflict between governmental authorities and organized armed groups or between such groups.[48] The term 'protracted' has been drawn from ICTY's jurisprudence as merely requiring some sort of duration of the hostilities, aimed at excluding civil unrest or terrorist activities from the ambit of the armed conflict.[49] ICC case-law seems to have excluded that the duration of the hostilities represents a distinct type of criteria envisaging a separate form of NIAC under paragraph (e). Conversely, when assessing the existence of a NIAC, the ICC's prosecution and Trial Chambers have considered exclusively the intensity of the armed conflict and the degree of the organization of the group, that should be sufficient to allow it to sustain protracted armed confrontations.[50]

In light of the above, in determining whether a NIAC involving cyber operations exists, the same criteria apply as for conventional armed violence.[51] Therefore, in order for a cyber operation conducted by NSA to fall within the ambit of article 8 para. 2 (c) to (f), it is necessary to prove that the operation reached a certain level of intensity and that the group satisfies a certain degree of organization. It appears reasonable to argue that only those operations that cause military harm to one of the belligerent parties, consisting for instance in physical damage to property, loss of life, injury to persons or significant disruption of critical infrastructure, could reach the intensity required to initiate a NIAC.[52] Indeed, with respects to the intensity criterion, isolated attacks conducted in absence of kinetic operations

---

46 Cottier, *op. cit.*, note 28, p. 313.

47 See, for instance, US Supreme Court, *Hamdan v. Rumsfeld*, 548 U.S. 65, 30 June 2006.

48 Rome Statute, Article 8(2)(f).

49 Cottier, *op. cit.*, note 28, p. 314; *Prosecutor v. Delalić.*, IT-96-21-T, Trial Chamber, Judgment, 16 November 1998, para. 184.

50 *See*, for instance, *Lubanga*, *op. cit.*, note 33, paras. 534-538; *Prosecutor v. Katanga*, ICC-01/04-01/07-3436-tENG, Trial Chamber, Judgment, 07 March 2014, paras. 1183-1187; *Prosecutor v. Bemba*, ICC-01/05-01/08-3343, Trial Chamber, Judgment, 21 March 2016, paras. 134-140. See, in general, ICRC *Commentary*, *op. cit.*, note 45.

51 Schmitt, *op.cit.*, note 9, pp. 385-391.

52 Dinniss, *op. cit.*, note 34, pp. 129-131; Roscini, *op. cit.*, note 35.

would be excluded from qualifying as a NIAC, even in cases where these attacks cause significant material harm and destruction, including loss of life.[53] It goes without saying that it is not likely that disruptive cyber operations that do not cause destruction would meet the criterion.[54] For instance, the Experts in the Tallinn Manual 2.0 exclude that "network intrusions, the deletion and destruction of data (even on a large scale), computer network exploitation, and data theft" amount to a NIAC, as would not mere blocking of functions and services, and defacing of websites.[55] However, among the Experts there was no consensus as to whether non-destructive cyber operations that are conducted during internal disturbances or alongside other acts of violence that alone are insufficient to qualify as a NIAC by organized armed groups could, however severe, be considered in order to fulfil the intensity criteria and trigger a NIAC.[56]

However, if we assume that a cyber operation fulfils the intensity criterion, the organization criterion would be even more difficult to prove in case of private individuals or loosely affiliated groups of hackers and online collectives. The organization of the parties involved in the hostilities, which has to be assessed on factual circumstances and determined on a case-by-case basis,[57] has been typically inferred from the existence of an effective command structure capable of coordinating military activities and determining a unified military strategy, as well as the group's capacity to conduct large-scale military operations.[58] Although online col-

---

53 See also Gisel, L., *et al.*, *op. cit.*, note 7, p. 305 ("while arguably not impossible in exceptional circumstances, it will be unlikely that cyber operations alone would meet the intensity requirement for a non-international armed conflict").

54 Schmitt, *op.cit.*, note 9, pp. 105-106; Dinniss, *op. cit.*, note 34, p. 131 (arguing that if an armed group launches a protracted series of attacks intended to cause physical damage to life and/or property, regardless of their kinetic or cyber nature, these acts would, under the ICRC interpretation, be considered the start of an armed conflict).

55 Schmitt, *op. cit.*, note 9, p. 388.

56 *Ibid*, p. 389. The view that cyber operations need to cause physical damage and injury, and to a certain extent potentially incapacitation, in order to reach the intensity level required by NIACs was also shared by the Council of Advisers in the Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare. See, The Permanent Mission of Liechtenstein to the United Nations, The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare, 2021, [https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf] Accessed February 2023.

57 *Prosecutor v. Limaj et al.*, IT-03-66-T, Trial Chamber, Judgment, 30 November 2005, para. 90 (in determining the organization of the Kosovo Liberation Army, the Trial Chamber considered for instance "factors including the existence of headquarters, designated zones of operation, and the ability to procure, transport, and distribute arms"). A group can be considered "armed", if it has the capacity to launch lethal or destructive cyber attacks. Schmitt, *op.cit.*, note 9, p. 389.

58 Conversely, it is not necessary that the group possesses a "conventional militarily disciplined unit". *See* Schmitt, *op.cit.*, note 9, p. 389; *Limaj*, TC Judgment, *op. cit.* 57, paras. 129-132.

lectives operating in cyberspace such as Anonymous appear to be driven by common causes and objectives, as in the case of the Russian/Ukrainian armed conflict when they shared forces against the Russian government, and their activities and targets are at least discussed among their members, their level of organization is questioned.[59] Their loose structure, the absence of a spokesperson or a chain of command, as well as of any sort of internal regulations or headquarters (these groups normally organize themselves online, and never meet)[60], would exclude that they are considered an organized armed group within the meaning of IHL.[61]

Of course, these considerations would not apply to armed groups with a sufficient degree of organization such as to enable them to implement and respect IHL and to carry out sustained and protracted attacks (both kinetic and cyber). In that case, IHL would apply and their members could be punishable for possible war crimes under the Rome Statute.[62] However, things would be different in case of armed groups with some degree of hierarchical structure, but who never met in person: in such a situation, the organization requirement would be difficult to prove.[63]

In conclusion both the intensity and the organization criteria would be challenging to meet in case of sporadic cyber operations by either private individuals or "hacktivist" groups, and IHL would not apply.[64] Conversely, their actions would be regulated by domestic criminal law and human rights law.[65]

---

59 Buchan, *op. cit.*, note 22, pp. 741-742.

60 Nevertheless, the majority of the Experts in the Tallinn Manual argue that the fact that these groups never met in person does not alone represent a ground to exclude altogether the organization requirement. Schmitt, *op.cit.*, note 9, p. 390.

61 On the organized armed group requirement, and the difficulty of applying it to digital groups, see for instance: Beatty G., *War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute*, The Military Law and the Law of War Review, Vol 58, No.2., 2020, p. 227. The majority of the Experts of the Tallinn Manual agreed that informal groups who operate "without any coordination" – i.e. without an informal leadership entity capable of directing the group's activities, identify potential targets, and maintaining an inventory of tools – would not satisfy the organization requirement, even if they shared a common goal. Schmitt, *op.cit.*, note 9, pp. 390-391.

62 Of course, in the case at hand, in order for the ICC to exert its jurisdiction, the other requisites shall also apply, i.e. the conduct shall fulfil the elements of Article 8 (both the mental and the material element), it shall be considered admissible under Article 17, and it shall take place in the territory of or by a national of a State party to the ICC Statute or a State that has accepted its jurisdiction.

63 The Experts in the Tallinn Manual were divided as to whether a "virtual armed group" would satisfy the organization requirement, "since there would be no means to implement the law with regard to individuals with whom there is no physical contact". Schmitt, *op. cit.*, note 9, p. 390.

64 Beatty, *op. cit.*, note 61, p. 227.

65 Schmitt, *op. cit.*, note 36, pp. 105-106.

3.2. The cyber operation must be sufficiently grave under Article 17 of the Rome Statute

Being the ICC a Court of last resort,[66] Article 17 of the Rome Statute imposes that in order for a case to be admissible, it must be "of sufficient gravity to justify further action by the Court".[67] Similarly, under Article 53, in deciding whether or not initiating an investigation or to proceed to a prosecution, the Prosecutor shall consider, *inter alia*, the gravity of the crime and the admissibility requirements under Article 17.[68]

Neither the Rome Statute nor its drafting history provide for criteria that should be used for the assessment of the gravity requirement.[69] The Office of the Prosecutor (OTP) and the Pre-Trial Chamber (PTC) have based their evaluation of the gravity requirement on two elements. On the one side, the gravity assessment included an evaluation of a series of factors, including the systematic nature of the conduct (i.e., the pattern of incidents), and the social alarm that the conduct(s) may have caused in the international community. On the other side, gravity has additionally been considered in light of the position of persons involved, including those who were the "most responsible" for the alleged systematic or large-scale commission of crimes.[70]

With respect to the first element, in the 2013 Policy Paper on Preliminary Examinations, the OTP has acknowledged that – provided that any crime that falls within the jurisdiction of the Court shall be serious in nature[71] – its assessment of

---

66 Contrary to the International *ad hoc* Criminal Tribunals for the Former Yugoslavia (ICTY) and for Rwanda (ICTR), which had primacy over domestic jurisdictions, the ICC shall be complementary with respect to national criminal jurisdiction and shall exercise its jurisdiction over cases when the State(s) that normally would have jurisdiction over it, is (are) unwilling or unable to carry out effective investigations or prosecutions. Rome Statute, Articles 1 and 17.

67 Rome Statute, Article 17(d).

68 Such evaluation must be done in the preliminary examinations under Article 53(1)(b), and during the investigations as a condition to begin the actual prosecution under Article 53(2)(b). Rome Statute, Article 53 para. 1(b)(c), para. 2(b)(c).

69 On the admissibility test pursuant to Article 17, see for instance: Werle, G.; Jeßberger, F., *Principles of International Criminal Law*, 4th Edition, Oxford University Press, Oxford, 2020, paras. 344-353. *See*, also, Roscini, M., *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*, Criminal Law Forum, Vol. 30, 2019, pp. 255 *et seq*.

70 *Prosecutor v. Lubanga,* ICC-01/04-01/06-1-Corr-Red, Decision on the Prosecutor's Application for a warrant of arrest, Article 58, 10 February 2006, paras 42 *et seq*.

71 See, Rome Statute, Preamble, Article 1, Article 5.

gravity includes both quantitative and qualitative considerations.[72] These include the scale, the nature, the manner of commission of the crimes, and their impact.

The scale refers to the number of victims, as well as to the harm imposed to them and to their families, to the extent of the damage or the geographical or temporal scale of crimes (the intensity might also be considered). In the interpretation of scale, the AC of the ICC clarified, however, that Article 8(1) does not impose a fixed requirement on war crimes to be part either of a plan or policy or of a large-scale commission to be admissible under Article 17.[73]

The nature of the crimes relates to specific elements of offences, which may be deemed of greater concern, for instance "killings, rapes and other crimes involving sexual or gender violence and crimes committed against children, persecution, or the imposition of conditions of life on a group calculated to bring about its destruction".[74]

The manner of commission considers for instance the existence of a plan or organized policy, the way the crimes were committed, or if they involved cruelty, as well as the vulnerability of the victims.[75]

Lastly, the terror or the sufferings inflicted on victims, as well as the social and environmental damage could be elements contributing to the impact as a factor to assess the gravity of a crime.[76]

Up until now, it does not seem that the cyber operations, especially when conducted by NSAs, have resulted in serious humanitarian consequences, their actions being limited to DDoS attacks or ransomwares. These "only result in temporary and reversible harm to the target" which "might lead to the temporary interruption of services but not physical damage of persons or property".[77] Therefore, to the current situation, it appears that it is unlikely that cyber operations conducted by NSAs would be grave enough to trigger the ICC's jurisdiction. According to Roscini, cyber operations could satisfy the gravity threshold if, for instance, they are characterized by cruelty (i.e. they may consist in a change in medical records,

---

72 ICC, Office of the Prosecutor, *Policy Paper on Preliminary Examinations*, November 2013, paras. 59 *et seq*.

73 ICC, *Situation in the Democratic Republic of the Congo*, ICC-01/04-169, Appeals Chamber, Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled "Decision on the Prosecutor's Application for Warrants of Arrest, Article 58", 12 July 2006, paras. 70-71.

74 OTP, 2013 Policy Paper, *op. cit.*, note 72, para. 63.

75 *Ibid.*, para. 64.

76 *Ibid.*, para. 65.

77 Roscini, *op. cit.*, note 68, p. 263.

so that patients receive unnecessary treatment), or if they have significant impact or serious repercussions on national infrastructures, for instance by disrupting the provision of essential services to the population or causing damage to the natural environment, or if they target specially protected persons.[78]

With respect to the second element of gravity assessment relating to the persons involved, the Prosecutor and the PTC in the *Mavi Marmara* situation disagreed on how to identify those "most responsible" for the commission of the alleged crimes. By dismissing the position of the OTP, i.e. that the "most responsible" referred to senior military commanders and political leaders, the judges of the PTC argued that it rather referred to those persons who may "bear the greatest responsibility" for such crimes, regardless of their seniority or hierarchical positions.[79] In determining the individual criminal responsibility for cyber operations, the rank or other forms of leadership could be difficult to establish, or it "may give way to more horizontal structures and dynamics that depend more on cyber skills and (enemy) vulnerabilities than the capacity to command and control".[80] According to Roscini, individuals who operate in cyberspace may play different roles, which range from the material execution of the cyber attack, to the development of the malware used, or the recruitment and training of hack-

---

78 *Ibid.*, p. 266.

79 On 14 May 2013, the Government of the Union of the Comoros referred to the OTP a situation relating to an Israel raid on the Humanitarian Aid Flotilla bound for the Gaza strip. With a decision of 6 November 2014, the Prosecutor announced her decision not to investigate the incident and to close the preliminary examination, in particular on the grounds of insufficient gravity pursuant to articles 17(1)(d) and 53(1)(b) of the Statute. On 16 July 2015, following a request for the review of the decision by the Government, the PTC requested the OTP to reconsider the decision, by ruling that the Office erred in the assessment of gravity. On 6 November 2015, the Appeals Chamber, by majority, rejected the OTP's appeal against the decision of the PTC. After two years, on 29 November 2017, the Prosecutor reaffirmed her previous view that the information available did not provide a reasonable basis to proceed with an investigation. On 2 September 2019, the AC dismissed the Prosecutor's appeal against the decision of the PTC, which had ruled that she had to reconsider her decision. On 16 September 2020, the PTC rejected the Government's application for judicial review and decided not to request the Prosecutor to reconsider her decision. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia*, Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation, Pre-Trial Chamber I, ICC-01/13-34, 16 July 2015, paras. 23-24; Decision on the admissibility of the Prosecutor's appeal against the "Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation", Appeals Chamber, ICC-01/13 OA, 6 November 2015; Notice of Prosecutor's Final Decision under Rule 108(3), ICC-01/13, Pre-Trial Chamber, 29 November 2017; Judgment on the appeal of the Prosecutor against Pre-Trial Chamber I's 'Decision on the "Application for Judicial Review by the Government of the Union of the Comoros"', ICC-01/13 OA 2, 2 September 2019; Decision on the 'Application for Judicial Review by the Government of the Comoros', Pre-Trial Chamber I, ICC-01/13, 16 September 2020.

80 Saxon, D., *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 570-571.

ers, or provide the necessary information of a target. In these cases, they may be involved as co-perpetrators or accessories.[81] Moreover, individuals may also be criminally responsible for the employment of cyber operations used in order to instigate, aid, abet, or otherwise assist the commission of a crime carried out "traditionally" and be liable under Article 25(b)-(d) of the Rome Statute.[82] However, in the cyberspace scenario, which is characterized by anonymity, it may be extremely difficult to identify the "most responsible person" for the alleged commission of a crime.[83]

3.3. The cyber operation must fulfil the elements of war crimes under Article 8

When dealing with the application of the Rome Statute to cyber operations, IHL principles become of particular importance, namely those referring to distinction, proportionality, and precaution, as it is generally acknowledged that cyber operations specifically relate to targeting.

It is usually argued that only those cyber operations that amount to an "attack" within the meaning of Additional Protocol I can be subject to the application of IHL's principles and therefore constitute war crimes.[84] It is common ground that the notion of attack quite indisputably extends to those cyber operations "reasonably expected to cause injury or death to persons or damage or destruction to objects", but also serious illness and severe mental suffering equivalent to injury.[85] The causal effects are not limited to the direct consequences that an attack may cause on the targeted cyber system, but also include the consequential damage, destruction, injury or death that can be foreseen.[86] The example provided by the Experts in the Tallinn Manual includes the remote manipulation of a Supervisory Control and Data Acquisition (SCADA) system of a dam that results in the release of waters and consequential extensive downstream destruction and harm to individuals, without necessarily damaging the system itself.

---

81 Roscini, *op. cit.*, note 68, pp. 256-257.

82 Schmitt, *op.cit.*, note 9, pp. 395-396.

83 Roscini, *op. cit.*, note 68, p. 258.

84 Additional Protocol I, Article 49(1) (defining attacks as "acts of violence against the adversary, whether in offence or defence").

85 Schmitt, *op.cit.*, note 9, pp. 415 (also noting that "*de minimis* damage or destruction does not meet the threshold of harm required by [Rule 92]", and that "[n]on-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks"), p. 417.

86 *Ibid.*, p. 416.

Against this background, cyber attacks that target civilians[87] and civilian objects,[88] or that are indiscriminate in nature,[89] or that cause excessive incidental loss of life, injury or damage to civilians[90] are prohibited under IHL and may constitute war crimes.[91]

A more controversial issue is represented by cyber operations that do not result in physical damage, but that negatively affect the functionality of infrastructure. Although views differ, in general terms it may be argued that the interpretation of the notion of attack could also encompass those cyber operations that do cause a loss of function or which significantly disrupt a system, for instance by disabling a computer or a network, although they may not necessarily amount to a war crime.[92] The Experts in the Tallin Manual, for instance, were divided: while some of them excluded that mere interference with the functionality of an object amounts to damage or destruction, the majority argued that it does, to the extent that such interference with functionality requires a replacement of physical components, or reinstallation of the operating system or of particular data.[93] Moreover, according to the view of some of them, a cyber operation that manipulates, alters, or deletes specific data that cause a cyber infrastructure not to perform its intended functions, would amount to an attack as well.[94]

---

87 Pursuant to the principle of distinction, "[t]he civilian population as such, as well as individual civilians, shall not be the object of cyber attack". *Ibid.*, pp. 422-423.

88 *Ibid.*, pp. 434-435 ("Civilian objects shall not be made the object of cyber attacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective").

89 *Ibid.*, pp. 455-457 ("It is prohibited to employ means or methods of warfare that are indiscriminate by nature", i.e., "(a) when they cannot be directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction").

90 Pursuant to the principle of proportionality, a "cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited". *Ibid.*, pp. 470-476.

91 *Ibid.*, p. 391.

92 The Council of Adviser adopts the view that Article 8's provisions deriving from IHL core principles only applies to "attacks" for the purposes of IHL, although underlining that neither the Elements of Crimes nor the ICC Statute do actually define them. Council of Advisers, *op. cit.*, note 56, pp. 37-39; Droege, *op. cit.*, note 7, p. 559 ("an attack must also be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary"); Ambos, K., *International criminal responsibility in cyberspace*, in: Tsagourias, N.; Buchan, R. (eds.), Research Handbook on International Law and Cyberspace, 2015, p. 124 ("a cyber operation leaving the targeted object physically intact but neutralizing it in its functionality may amount to a militarily relevant attack, at least if the operation disables the 'critical infrastructure' of the respective State", footnotes omitted).

93 Schmitt, *op.cit.*, note 9, p. 417.

94 *Ibid.*, p. 418.

It is debated whether the deletion or alteration of data could be considered an attack even in absence of resulting damage or loss of functionality of the cyber infrastructure. Against the position of the Tallinn Manual on the issue (in which the majority of Experts excluded data from the category of objects protected under IHL due to their intangibility),[95] it is the opinion of several commentators that in view of the growing importance of data in digitized societies, civilian data are protected under IHL, and therefore their alteration and deletion could possibly be considered a violation of IHL, in particular when essential civilian data are involved.[96] Some authors indeed advocate for a progressive interpretation of the notion of "object" and "property" under the Rome Statute so as to include – under some conditions – certain categories of civilian data under the scope of protection offered by IHL, in light of the importance of protecting civilians and civilian objects from the effects of hostilities.[97]

On the other hand, it must be here also emphasized that it is the view of some commentators that disruptive cyber operations – i.e., those "actions that inter-

---

[95] There exists no definition of computer data under IHL instruments nor in the Rome Statute and States' practice on the issue is inconsistent. Scholars' views differ on whether to consider them as protected under IHL provisions, including in the Tallinn Manual, where not all Experts share the majority position that the notion of 'object' in international law of armed conflict shall not be interpreted as including data and that an attack on data *per se* does not constitute an attack under IHL. Instead, a minority of the Experts argues that data should be regarded as an object and protected from attack, in particular those which are deemed "essential to the well-being of the civilian population" such as "social security data, tax records, and bank accounts". Schmitt, *op.cit.*, note 9, p. 437.

[96] This "broader" view is also endorsed by the International Committee of the Red Cross, which considers 'essential civilian data' the "medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records". ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Policy paper, 28 November 2019 (ICRC 2019 Policy Paper), p. 8; Horowitz, J., *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, American Society of International Law, Vol. 24, Issue 11, 2020, [https://www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc#_ednref16] Accessed August 2023. On the debate, see also Gisel *et al.*, *op. cit.*, note 7, p. 317 (noting that, since "data is an essential component of the digital domain and a cornerstone of life in many societies", the interpretation and application of "IHL rules to safeguard essential data against destruction, deletion or manipulation will be a litmus test for the adequacy of existing humanitarian law rules").

[97] It must be noted that data belonging to medical units are protected, in light of the specific protection granted by IHL to medical facilities and personnel. ICRC 2019 Policy Paper, *op. cit.*, note 96, p. 8; Schmitt, *op.cit.*, note 9, p. 515. On the debate relating to the interpretation of the notion of "object" under IHL as including data, see for instance, McKenzie, S., *Civilian Operations against Civilian Data*, Journal of International Criminal Justice, Vol. 19, 2021 (arguing that, when it comes to the conceptualization of data, "the more straightforward and protective option would be to recognize data as part of a physical system that is capable of being attacked" and advocating for a 'progressive' approach by the ICC, which "would be more protective of civilian and could encourage the progressive development of ICL and IHL"), pp. 1181 – 1182; Horowitz, *op. cit.*, note 96; Mačák, K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, Israel Law Review, Vol. 48, No. 1, 2015, pp. 55 – 80.

rupt the flow of information or the functioning of information systems without causing physical damage or injury"[98] – may as well significantly affect the civilian population, for instance in the provision of essential services and in their access to basic need or they may undermine their fundamental human rights.[99]

Aside from the debate on what constitutes an "attack" in cyberwarfare, several offences listed in Art. 8 are indeed related to targeting and to the general prohibition on attacking particular protected targets, i.e. civilians[100] and civilian objects,[101] as well as personnel and objects involved in humanitarian assistance or peacekeeping missions or using distinctive emblems[102] or certain buildings or objects (e.g. dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected), provided they are not military objectives.[103] There is broad consensus over the fact that cyber operations that are intentionally[104] directed against civilians and cause civilian casualties, which destroy protected objects, or which are expected to cause excessive incidental loss of life or injury to civilians or damage to civilian objects or the natural environment do fall within the purposes of Article 8,[105] and therefore entail the individual criminal responsibility of the perpetrator(s).

When considering the participation of NSAs in cyberwarfare and their individual criminal responsibility under the Rome Statute, there exist a few issues that ought to be discussed.

First, the expansion of the notion of object as encompassing data whose deletion restriction or tampering could result in injury or damage to civilian objects could

---

98 Brown, G.; Tullos, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 2012, p. 115.

99 One example provided is the 2017 WannaCry ransomware attack, which had a great impact on the UK's National Health Service, by shutting down computers, cancelling appointments, diverting ambulances and impacting emergency services. Beatty, *op. cit.*, note 61, p. 216. It must be noted that, even in cases that a cyber operation does "not result in the requisite harm to the object of the operation", if it "cause[s] collateral damage", then such operation might amount to an attack, according to the views of the Experts in the Tallinn Manual. Schmitt, *op. cit.*, note 9, pp. 418-419.

100 Rome Statute, Article 8(2)(b)(i), Article 8(2)(e)(i).

101 Rome Statute, Article 8(2)(b)(ii). The same offence is not provided for under NIACs.

102 Rome Statute, Article 8(2)(b)(iii), Rome Statute, Article 8(2)(b)(xxiv), Article 8(2)(e)(ii).

103 Rome Statute, Article 8(2)(b)(ix), Article 8(2)(e)(iii and iv).

104 The mental element required under the Rome Statute is regulated by Article 30, which requires intent in relation to the conduct, and knowledge in relation to the consequence or awareness that it will occur in the ordinary course of events. Recklessness or negligence are not accepted. On the general issue of the *mens rea* required under the ICC, see for instance: Finnin, S., *Mental Elements under Article 30 of the Rome Statute of the International Criminal Court: A Comparative Analysis*, International and Comparative Law Quarterly, Vol. 61, Issue 2, 2012, pp. 325-359.

105 Rome Statute, Article 8(2)(b)(iv).

not be considered as applying to NIACs, since – under the Rome Statute – there appears to be no analogous crime that protects civilian objects (which are not military objectives) from attack. This necessarily implies that even if the ICC adopted a broad interpretation of what constitutes an "object" under IHL, thus justifiably expanding the protection to civilian data, in an armed conflict between a State and an organized armed group, or between organized armed groups – provided that the pre-requisites for the existence of the armed conflict are satisfied – there would be no provision applicable to an attack deliberately directed against civilian data. Nonetheless, attacks against civilian objects are prohibited and criminalized under international customary law and therefore any State could potentially prosecute the alleged responsible of the conduct.[106]

Similarly, while Article 8(2)(e)(i) criminalizes the conduct of "intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities" even in NIACs, two additional provisions prohibiting disproportionate and indiscriminate attacks cannot be found as applying to NIACs under the Rome Statute. Even in this case, the ICC Statute lags behind international customary law, where indiscriminate[107] and disproportionate attacks[108] are prohibited and criminalized both in IACs and NIACs. This

[106] Henckaerts, J.; Doswald-Beck L., (eds.) *Customary International Humanitarian Law*, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rule 7 ("The Statute of the International Criminal Court does not explicitly define attacks on civilian objects as a war crime in non-international armed conflicts. It does, however, define the destruction of the property of an adversary as a war crime unless such destruction be 'imperatively demanded by the necessities of the conflict'"). It must be noted that, during the Rome Conference, the customary status of the criminalization of the conduct of attacking civilian objects in NIACs appeared doubtful. However, it has been argued that the fact that a violation of the rule prohibiting attacks on civilian objects, when carried out with purposeful action, entails individual criminal responsibility can be deduced by the case-law of the ICTY. Werle; Jeßberger, *op. cit.*, note 69, paras. 1432-1433; *Prosecutor v. Kupreškić et al.*, IT-95-16-T, Trial Chamber Judgment, 14 January 2000, paras. 521 *et seq* (The protection of civilians in time of armed conflict, whether international or internal, is the bedrock of modern humanitarian law … Indeed, it is now a universally recognised principle, recently restated by the International Court of Justice [in the Nuclear Weapons case], that deliberate attacks on civilians or civilian objects are absolutely prohibited by international humanitarian law"; *Prosecutor v. Strugar*, IT-01-42-T, Trial Chamber, Judgment, 31 January 2005, paras. 224-226.

[107] *Ibid.*, Rule 11; *Tadić*, *op. cit.,* note 30, para. 134; *Prosecutor v. Kordić and Čerkez*, IT-95-14/2-PT, Trial Chamber, Decision on defence motion to dismiss the amended indictment for lack of jurisdiction based on the limited jurisdictional reach of articles 2 and 3, 2 March 1999, para. 31; *Kupreškić*, *ibid.*, para. 524.

[108] *Ibid.*, Rule 14. International customary law criminalizes the conduct of causing disproportionate incidental damage to civilians or civilian objects also in NIACs, as confirmed by State practice. Werle; Jeßberger, *op. cit.*, note 69, para. 1455; see also the Military manuals of Netherlands, Germany, Peru, Republic of Korea, Switzerland, available at ICRC Database, Customary IHL, *Practice relating to Rule 14, Proportionality in Attack*, [https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14] Accessed 10 March 2023.

means that, even if it is proved beyond reasonable doubt that NSAs are involved in a NIAC (hence that the organization requirement and intensity threshold are satisfied) and they do conduct cyber operations that are indiscriminate or disproportionate, an amendment to the Rome Statute should be required to expand the same protection that is granted to the civilian population in IACs also to NIACs.

To conclude, it should be emphasized that cyber operations could satisfy the material element of other offences, in addition to those relating to targeting. For instance, it has been discussed that cyber attacks carried out against nuclear power plants with the required *mens rea* may result in wilful killing under Article 8 (2) paragraphs (a)(i) and (c)(i), or violence to life or serious injury to body or health under paragraphs (a)(iii) and (c)(i).[109] Other authors suggest that the provision prohibiting the intentional starvation of civilian as a method of warfare under the Rome Statute[110] could encompass some forms of disruptive cyber operations.[111] In this last case too, however, the protection of civilians from the deprivation of objects indispensable to their survival would only apply to IACs before the ICC, in absence of analogous provisions applicable to NIACs in the Rome Statute.

4. CONCLUDING REMARKS

The possibility that NSAs such as cyber-criminals, transnational criminal groups, terrorist organizations, loosely affiliated bands of hackers or even isolated individuals perpetrate cyber-operations entails multiple concerns for the safety of civilians and civilian infrastructure. The anonymity and de-territorialization that typically characterize cyberspace by nature do affect the participation of States and NSAs to hostilities without distinction. However, in the case of NSAs, as discussed above, a series of additional challenges and concerns must be considered, especially when dealing with the application of the Rome Statute to cyber operations. These relate to the same existence of an armed conflict, which would require a certain level of intensity and organization that – at the moment – would be difficult to reach. Moreover, against the views of some commentators, disruptive cyber operations that do not cause material harm or physical damage, or loss of life or injury seem to be excluded from the application of IHL. The conducts of NSAs in cyberspace

---

109 Chaumette, A., *International Criminal Responsibility of Individuals in Case of Cyberattacks,* International Criminal Law Review, Vol. 18, 2018, pp. 14 – 15.

110 Rome Statute, Article 8(2)(b)(xxv), prohibiting the conduct of "[i]ntentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable to their survival, including wilfully impeding relief supplies as provided for under the Geneva Conventions" as a war crime applicable in IACs.

111 The author recalls that during negotiations non-food items such as medicines and blankets were mentioned as essential commodity or objects necessary to survival. Beatty, *op. cit.,* note 61, p. 234.

seem to be limited, for the moment, to DDoS attacks and ransomwares, which – absent a long-lasting tangible physical harm to persons or property – would hardly qualify as "attacks" under IHL nor would they trigger the ICC's jurisdiction.

However, it is imperative not to overlook or underestimate the potential cost of cyber operations conducted by NSAs and the grave consequences they may impose on civilians and civilian infrastructure. From this perspective, a comprehensive discussion regarding the application of ICC Statute provisions pertaining to war crimes must account for not only the challenges posed by conducts potentially amounting to war crimes in cyberspace but also, and with more difficulty, the involvement of NSAs in such operations and their individual criminal responsibility under international law. When faced with possible future examinations and investigations of situations and cases involving cyber operations, the ICC, and primarily the OTP and PTC should consider not only the admissibility issues, but also the statutory limits concerning war crimes. As things stand, Article 8 does not afford the same level of protection to civilians involved in NIACs as it does in IACs, especially those protecting civilian objects from attack or those protecting civilians from disproportionate and indiscriminate attacks. This could mean that, in the eventuality that the judges of the Court – if and when presented with conducts taking place in the cyberspace – adopted a broad interpretation of the notion of "object" so as to include data essential to the well-being of the civilian population, the same level of protection could not be afforded to civilians involved in NIACs.

Against this backdrop, whereas States could (and should) initiate proceedings against alleged perpetrators of war crimes by cyber means – namely in the cases where international customary law provides for a criminalization of the conducts discussed in the sections above and protects civilians and civilian objects, and provided domestic law is in line with international provisions –, States parties to the ICC should consider an amendment to the Rome Statute,[112] to limit the effects of hostilities on civilians as far as possible, regardless of the character of the armed conflict. More specifically, although the possibility of applying the Rome Statute provisions to cyber operations without needing to amend the Statute seem uncontested in legal doctrine, the absence of specific provisions prohibiting indiscriminate and disproportionate attacks, attacks against civilian objects, as well as the intentional starvation of civilians as a method of warfare as applying to NIACs necessarily limits the protection afforded to the civilian population from the adverse effects of hostilities.

[112] The amendment procedure of the Rome Statute is regulated by Articles 121 and 123 of the Rome Statute, under which any State Party may propose amendments also concerning the elements of crimes.

REFERENCES

BOOKS AND ARTICLES

1. Ambos, K., *International criminal responsibility in cyberspace*, in: Tsagourias, N.; Buchan, R. (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2015, pp. 118-143
2. Beatty G., *War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute*, The Military Law and the Law of War Review, Vol 58, No.2., 2020, pp. 209-239
3. Buchan, R., *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, Chinese Journal of International Law, 2016, Vol. 15, No. 4, pp. 741 – 772
4. Bussolati, N., *The Rise of Non-State Actors in Cyberwarfare*, in: Ohlin, J. D.; Govern, K.; Finklestein, C. (eds.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford University Press, 2015, pp. 102-126
5. Chaumette, A., *International Criminal Responsibility of Individuals in Case of Cyberattacks,* International Criminal Law Review, 2018, Vol. 18, pp. 1 – 35
6. Cottier, M., *Article 8, Part I: Introduction/General Remarks*, in: Triffterer O.; Ambos K. (eds.), The Rome Statute of the International Criminal Court: A Commentary, 3rd edition., C.H. Beck, Hart, Nomos, 2016
7. Dinniss, H., *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012
8. Droege, C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,* International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 533 – 578
9. Ducheine, P. A. L.; Pijpers B. M. J., *The notion of cyber operations*, in: Tsagourias N., Buchan, R. (ed.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2021, pp. 272-296
10. Finnin, S., *Mental Elements under Article 30 of the Rome Statute of the International Criminal Court: A Comparative Analysis*, International and Comparative Law Quarterly, Vol. 61, Issue 2, 2012, pp. 325 – 359
11. Gisel, L.; Rodenhäuser, T.; Dörmann, K., *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, in: International Review of the Red Cross, 2020, Vol. 102, No. 913, pp. 287 – 334
12. Henckaerts, J.; Doswald-Beck L., (eds.) *Customary International Humanitarian Law*, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005
13. Horowitz, J., *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, American Society of International Law, Vol. 24, Issue 11
14. Lin, H., *Cyber conflict and international humanitarian law*, International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 515 – 531
15. Mačák, K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, Israel Law Review, Vol. 48, No. 1, 2015, pp. 55 – 80
16. McKenzie, S., *Civilian Operations against Civilian Data*, Journal of International Criminal Justice, Vol. 19, 2021, pp. 1165 – 1192

17. Missiroli, A., *Present Tense: Cyber Defence Matters*, in: Pawlak, P; Delerue, F. (eds.), A Language of Power? Cyber Defence in the European Union, Chaillot Paper/176, November 2022
18. Roscini, M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014
19. Roscini, M., *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*, Criminal Law Forum, Vol. 30, 2019, pp. 247 – 272
20. Sassòli, M.; Bouvier, A.; Quintin, A., *How Does Law Protect in Law, Cases; Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, in: Outline of International Humanitarian Law (3rd ed.), International Committee of the Red Cross, 2012
21. Saxon, D., *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare*, Journal of Conflict & Security Law, Winter 2016, Vol. 21, No. 3, pp. 555 – 574
22. Schmitt, M., *Cyber Operations and the Jus in Bello: Key Issues*, International Law Studies, Vol. 87., 2011, pp. 89 – 110
23. Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017
24. Stiano, A., *L'intervento di Anonymous nel conflitto tra Russia e Ucraina: Alcune riflessioni sullo* status *giuridico degli* hacker *attraverso il prisma del diritto internazionale umanitario*, Ordine internazionale e diritti umani, No. 4, 2022, pp. 982 – 1000
25. Werle, G.; Jeßberger, F., *Principles of International Criminal Law*, 4th Edition, Oxford University Press, Oxford, 2020

INTERNATIONAL CRIMINAL COURT

1. *Prosecutor v. Bemba*, ICC-01/05-01/08-3343, Trial Chamber, Judgment, 21 March 2016
2. *Prosecutor v. Katanga*, ICC-01/04-01/07-3436-tENG, Trial Chamber, Judgment, 07 March 2014
3. *Prosecutor v. Lubanga,* ICC-01/04-01/06-1-Corr-Red, Decision on the Prosecutor's Application for a warrant of arrest, Article 58, 10 February 2006
4. *Prosecutor v. Lubanga*, ICC-01/04-01/06, Trial Chamber, Judgment, 14 March 2012
5. *Situation in the Democratic Republic of the Congo*, ICC-01/04-169, Appeals Chamber, Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled "Decision on the Prosecutor's Application for Warrants of Arrest, Article 58", 12 July 2006
6. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17, Pre-Trial Chamber II, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan, 12 April 2019
7. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17-138 OA4, Appeals Chamber, Judgment, 5 March 2020
8. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia*, ICC-01/13-34, Pre-Trial Chamber I, Decision on the request of the

Union of the Comoros to review the Prosecutor's decision not to initiate an investigation, 16 July 2015

9. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13 OA, Appeals Chamber, Decision on the admissibility of the Prosecutor's appeal against the "Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation", 6 November 2015
10. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13, Pre-Trial Chamber, Notice of Prosecutor's Final Decision under Rule 108(3), 29 November 2017
11. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13 OA 2, Appeals Chamber, Judgment on the appeal of the Prosecutor against Pre-Trial Chamber I's 'Decision on the "Application for Judicial Review by the Government of the Union of the Comoros"', 2 September 2019
12. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13, Pre-Trial Chamber I, Decision on the 'Application for Judicial Review by the Government of the Comoros', 16 September 2020

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA

1. *Prosecutor v. Delalić.*, IT-96-21-T, Trial Chamber, Judgment, 16 November 1998
2. *Prosecutor v. Kordić and Čerkez*, IT-95-14/2-PT, Trial Chamber, Decision on defence motion to dismiss the amended indictment for lack of jurisdiction based on the limited jurisdictional reach of articles 2 and 3, 2 March 1999
3. *Prosecutor v. Kunarac et al.,* IT-96-23 & IT-96-23/1-A*,* Appeals Chamber, Judgment, 12 June 2002
4. *Prosecutor v. Kupreškić et al.*, IT-95-16-T, Trial Chamber Judgment, 14 January 2000
5. *Prosecutor v. Limaj et al.*, IT-03-66-T, Trial Chamber, Judgment, 30 November 2005
6. *Prosecutor v. Strugar*, IT-01-42-T, Trial Chamber, Judgment, 31 January 2005
7. *Prosecutor v. Tadić*, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995

INTERNATIONAL DOCUMENTS

1. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S. 31
2. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S. 85
3. Geneva Convention Relative to the Treatment of Prisoners of War Aug. 12, 1949, 75 U.N.T.S. 135
4. Geneva Convention Relative to the Protection of Civilian Persons in Times of War, Aug. 12, 1949, 75 U.N.T.S. 287
5. International Criminal Court, Elements of Crimes, 2011, ISBN No. 92-9227-232-2

6. Office of the Prosecutor, *Policy Paper on Preliminary Examinations*, Policy Paper, November 2013
7. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 U.N.T.S. 3
8. UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. US Supreme Court, *Hamdan v. Rumsfeld*, 548 U.S. 65, 30 June 2006

REPORTS

1. Gisel L.; Olejnik, L. (eds.), *The potential human cost of cyber operations*, International Committee of the Red Cross, Report, 2018
2. International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts - Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, Report, 2019
3. International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Policy paper, 2019

WEBSITE REFERENCES

1. Ambos, K., *Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Ambos], Accessed 20 February 2023
2. Brown, G., Tullos, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 2012, [https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations], Accessed February 2023
3. Cerulus L., *Kyiv's hackers seize their wartime moment*, Politico, 2022, [https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/], Accessed November 2022
4. Costello, R. Á., *Facilitating the Use of Open Source Evidence at the International Criminal Court: Authentication and the Problem of Deepfakes*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence#Costello], Accessed 15 November 2022
5. Goodin, D., After *Ukraine recruits an "IT Army," dozens of Russian sites go dark*, Arstechnica, 2022, [https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/], Accessed November 2022
6. Holland, S., Pearson, J., *US, UK: Russia responsible for cyberattack against Ukrainian banks*, Reuters, 2022, [https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/], Accessed November 2022
7. ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949, Commentary of 01.01.2020,

Article 3 - Conflicts not of an international character, [https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020], Accessed February 2023

8. ICRC Database, Customary IHL, Practice relating to Rule 14, Proportionality in Attack, [https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14], Accessed 10 March 2023
9. Johnson, B., *Hackers Turn Conti Ransomware Against Russia as Twitter Suspends Some Anonymous Accounts*, HomelandSecurity Today, 2022, [https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-turn-conti-ransomware-against-russia-as-twitter-suspends-some-anonymous-accounts/], Accessed November 2022
10. Koloßa, S., *The Dangers of Hacktivism How Cyber Operations by Private Individuals May Amount to Warfare*, 2022, [https://voelkerrechtsblog.org/the-dangers-of-hacktivism/], Accessed 04 February 2023
11. Milmo, D., *Anonymous: the hacker collective that has declared cyberwar on Russia*, The Guardian, 2022, [https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia], Accessed November 2022
12. Roscini, M., *Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute*, ICC Forum, 2022,, [https://iccforum.com/cyberwar#Roscini], Accessed November 2022
13. Schectman, J., Bing, C., *Ukraine calls on hacker underground to defend against Russia*, Reuters, 2022, [https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/], Accessed November 2022
14. Schmitt, M., N., Biggerstaff, W., C., *Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating In Hostilities?,* 2022, [https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/], Accessed 20 February 2023
15. Schmitt, M., N., *Ukraine Symposium – Using Cellphones To Gather and Transmit Military Information, A Postscript*, 2022, [https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/], Accessed 20 February 2023
16. The Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*, 2021, [https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf], Accessed February 2023.
17. *To What Extent Can Cyber Evidence Repositories, and Digital and Open-Source Evidence, Facilitate the Work of the OTP, and the ICC More Generally?*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence], Accessed 15 November 2022
18. *Who is Squad303 that is attacking Russia with Text Messages*, The Tech Outlook, 2022, [https://www.thetechoutlook.com/news/new-release/software-apps/who-is-squad303-that-is-attacking-russia-with-text-messages/], Accessed November 2022

UDK 349.23-054.6:341.9
Original scientific paper

CONTEMPORARY FORMS OF WORK WITH A DIGITAL FEATURE IN PRIVATE INTERNATIONAL LAW*

Jura Golub, LLM, Research Assistant
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
jgolub@pravos.hr

ABSTRACT

Digitalization has enabled the rapid development of the gig economy and changed the entire paradigm in such a way that through digitalization people are increasingly achieving their primary employment. As a result, there is a frequent occurrence of the phenomenon of digital nomads and platform workers. Although initially conceived as freelance jobs, in certain cases, the legal relationships of digital nomads or platform workers take on the characteristics of an employment relationship. To circumvent fiscal and labour obligations, digital nomads or platform workers are often defined in contracts as self-employed individuals or independent contractors, resulting in a deprivation of labour rights. Consequently, a challenge arises for European private international law in terms of the correct characterization regarding the legal relationship and, subsequently, the application of the appropriate conflict of law rule to determine the applicable law.

Keywords: *applicable law, characterization, digitalization, digital nomads, platform work, private international law*

1. INTRODUCTION

The development of information and communication technologies has caused changes in various spheres of social life. The exception to the above is not even the field of work in which digitalization has contributed to a paradigm shift in labour

* 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. This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. ORCID: [https://orcid.org/0000-0002-2440-8081].

relations with the emergence of atypical forms of work. Although the gig economy as a phenomenon has been present for a long time, due to the flexibility of the contractual conditions for both contracting parties, it has taken on a completely new dimension with digitalization. This new dimension of the gig economy is most evident in the field of digital labour platforms, which use digital technologies to connect workers and clients to perform individual tasks, that is on a per task basis.[1] Parallel to that, also with ubiquitous digitization, the phenomenon of digital nomads is also developing, but with the essential feature of international mobility of service providers.

In this sense, the emergence of platform workers and digital nomads presents new challenges to private international law. The key problem is the proper characterization of the legal relationship between platform workers / digital nomads and the other contracting party. Is it an employment relationship or some other contractual relationship? Namely, the work of digital nomads/platform workers can be characterized as an employment relationship or the work of a self-employed person. However, in the gig economy it is common practice to classify workers as service providers rather than employees in contracts.[2] According to the European Commission's estimate, in 2021 more than 28 million people worked for digital work platforms, and it is estimated that by 2025 that number will reach 43 million people. [3] However, the European Commission also estimates that at least 5.5 million people are misclassified as "self-employed".[4] As a result of the aforementioned misclassification, "self-employed" persons are deprived of numerous labour rights inherent in European legal tradition that they would have enjoyed if their status had been properly classified as an employment relationship.

Besides proper characterization, an additional challenge encountered in private international law pertains to the localization of legal relationships with international element. This challenge is particularly pronounced when dealing with platform workers and digital nomads, wherein a notable characteristic is their mobility facilitated by digital technologies. Consequently, these individuals can carry out their work from various locations worldwide, changing them frequently. Hence,

---

1 Van Calster, G., *Of giggers and digital nomads – what role for the HCCH in developing a regulatory regime for highly mobile international employees*, in: John, T., Gulati, R., Köhler, B. (eds.), The Elgar Companion to the Hague Conference on Private International Law, Edward Elgar Publishing, Cheltenham and Northampton, 2020, p. 464.

2 *Ibid*.

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better working conditions for a stronger social Europe: harnessing the full benefits of digitalisation for the future of work COM/2021/761 final, pp. 5-6.

4 *Ibid*.

it is of importance to localize the legal relationships involving platform workers/digital nomads and determine the actual seat (*situs*) of such relationships. This is essential for the correct determination of the applicable law, considering that these individuals have the ability to frequently change their work locations.

Therefore, it arises as a research question, under what assumptions can platform workers and digital nomads be considered employees in the sense of European private international law (EU PIL)? Accordingly, this contribution aims to: 1) determine the legal status of platform workers and digital nomads in accordance with the EU PIL; and 2) determine applicable law for legal relationships involving platform workers and digital nomads, under the hypothesis that it is an employment relationship.

To address the aforementioned issues and achieve the research objectives, this contribution will first define the concepts of platform work and digital nomadism. In the subsequent step, the characterization of legal relationships involving platform workers and digital nomads will be examined to determine the conditions under which they can be classified as employees within the context of EU PIL. Lastly, this contribution will consider questions pertaining to applicable law for legal relationships involving platform workers and digital nomads, assuming that they involve individual employment contracts.

Certainly, matters of jurisdiction in disputes involving platform workers or digital nomads are also deserving of attention. However, given the scope of this topic, questions of jurisdiction will be addressed in future research, while this contribution primarily focuses on issues related to applicable law.

2. DEFINING THE CONCEPTS OF PLATFORM WORKERS AND DIGITAL NOMADS

The emergence of platform work signifies a novel form of labour, whereby digital infrastructure facilitates the connection between the demand and supply of specific services, while also organizing their execution through platform guidelines and user feedback.[5] Moreover, algorithmic governance plays an increasingly ubiquitous role in terms of a substitute for conventional supervision by the employer.[6] The fundamental characterization of platform workers is considered from the perspective of the location of their work. Thus, platform workers are distinguished

[5] Aloisi, A., *Platform Work in the EU: Lessons learned, legal developments and challenges ahead*, European Commission, Brussels, 2020, p. 1.

[6] *Ibid*.

based on whether they perform offline activities or online activities.[7] Offline activities of platform workers pertain to providing on-demand services through an application, typically involving services such as transportation, delivery, or household work. These activities, however, require work to be carried out in a physical or geographically specific location.[8] On the other hand, platform workers engaged in online activities perform their work exclusively within a virtual environment, irrespective of the geographical location of their work. This category of work is commonly referred to as „crowdwork".[9]

In the context of EU PIL and platform work, according to *Vukorepa*, the following typology of performing platform work with a cross-border element is possible: 1) the platform worker performs work from one Member State for the platform or a user in another Member State; 2) the platform worker physically relocates to another Member State; and 3) the platform worker is simultaneously employed in multiple Member States.[10] In general, based on their function, two types of digital platforms can be distinguished. The first category of digital platforms is those that provide information society services.[11] The function of such platforms is solely to mediate between users, i.e., between service providers and service recipients.[12] In simplified terms, the platform fulfills its purpose by connecting the service provider and the service recipient, who then directly enter into a contract.[13] The opposite category of digital platforms is those platforms that, in addition to their mediating function, also perform additional functions such as payment process-

---

7 Boto, J. M. M., *Collective Bargaining and the Gig Economy: Reality and Possibilities*, in: Boto, J. M. M. and Brameshuber, E. (eds), Collective Bargaining and the Gig Economy, Hart Publishing, Oxford, 2022, pp. 3-4.

8 Weiss, M., *The platform economy. Tha main challenges for labour law*., in: Mella Mendez, L. (ed.), Regulating the Platform Economy. International Perspectives on New Forms of Work, Routledge, Oxon and New York, 2020, p. 12.

9 Boto, *op. cit.*, note 7, pp. 3-4.

10 Vukorepa, I., *Prekogranični platformski rad: zagonetke za slobodu kretanja radnika i koordinaciju sustava socijalne sigurnosti*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 70, No. 4, 2020, pp. 489-490.

11 According to art. 1(1)(b) of the Directive (EU) 2015/1535 of the European parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), that kind of service is normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

12 Tereszkiewicz, P., *Digital Platforms: Regulation and Liability in EU Law*, in: DiMatteo, L. A., Cannarsa, M., and Poncibò, C. (eds) The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge University Press, Cambridge, 2019, p. 146.

13 Gruber-Risak, M., *Classification of Platform Workers: A Scholarly Perspective*, in: Gyulavári, T. and Menegatti, E. (eds), Decent Work in the Digital Age, European and Comparative Perspectives, Hart Publishing, Oxford, 2022, p. 86.

ing and monitoring of the services provided by the service provider.[14] In this case, a tripartite legal relationship arises between the platform worker, the platform, and the end user.[15] In the context of platform workers in legal situations with international characteristics, this contribution will consider the second category of digital platforms. In such a tripartite relationship, attention is drawn to the specific relationship between the platform worker and the platform itself, given the supervision exercised by the platform over the worker's activities. This raises a legal question of whether the platform worker is truly a self-employed individual who autonomously makes decisions about how to conduct their business activities, as often classified by the contracting parties, or whether the platform worker is an employee of the digital platform, regardless of the classification of the legal relationship between the contracting parties.[16]

On the other hand, the concept of digital nomads may or may not align with the characteristics of platform workers. The concept of digital nomads can be simplest defined as a lifestyle that combines the advantages of modern information and communication technologies with continuous mobility worldwide.[17] Thanks to a combination of gig work and digital platforms, digital nomads work in various locations around the world.[18] For digital nomads, a stable Internet connection is crucial, as they typically deliver their work results, performed from various parts of the world, via the Internet.[19] In the context of private international law, it is characteristic of the concept of digital nomads that they work, either as employees or self-employed individuals, from the country where they are temporarily located for an employer or client located in another country, rather than in the host country.[20] It is incorrect to equate digital nomads who are in an employment relationship with an employer in another country solely because they perform their work in a different country from where the employer is located. In the case of posted workers, the initiative for work in another country always comes from the employer with a strictly limited duration, representing temporary work in

14 Tereszkiewicz, *op. cit.*, note 12, p. 146-147.

15 Gruber-Risak, *op. cit.*, note 13, p. 86.

16 Weiss, *op. cit.*, note 8, pp. 12-13.

17 Chevtaeva, E., Denizci-Guillet, B., *Digital nomads' lifestyles and coworkation*, Journal of Destination Marketing & Management, Vol. 21, 2021.

18 Richter, S. and Richter, A., *Digital Nomads*, Business & Information Systems Engineering, Vol. 62, 2020, p. 79.

19 Brown, N., *Law, Jurisdiction and the Digital Nomad: Why we need more appropriate mechanisms for determining sovereignty over disputes*, Computer Law Review International, Vol. 16, No. 2, 2015, p. 38.

20 Bruurs, S., *Digital Nomads and the Rome I Regulation: An Overview*, Global Workplace Law & Policy, 2022, p. 2, [https://global-workplace-law-and-policy.kluwerlawonline.com/2022/12/14/digital-nomads-and-the-rome-i-regulation-an-overview/], Accessed: 15 April 2023

the host country.[21] Of course, in the case of an employment relationship, digital nomadism will only be possible if the employee and the employer agree on the freedom to choose the place of work, meaning that the physical presence of the employee at a specific location determined by the employer is not expected. When choosing their location, digital nomads typically opt for exotic destinations or even combine stays in one country during the winter months with stays in another country during the summer months.[22] It should be noted that it would be incorrect to equate digital nomads with tourists. Digital nomads continuously balance between professional productivity and travel.[23]

Given the observed phenomenon of digital nomads, many European and other countries have introduced digital nomad visas that allow digital nomads and their family members to have a longer lawful stay of a temporary nature in the host country. However, typically, these visas do not grant access to the domestic labour market because digital nomads are expected to carry out remote work using digital technology.[24] As a result, various legal definitions of digital nomads can be found in different legislations. For example, Croatian immigration law defines digital nomads as third-country nationals (non-EU citizens) who are employed or perform work through communication technology for a company or their own company that is not registered in Croatia.[25] An additional requirement under Croatian law is that digital nomads do not provide services to employers in Croatia.[26] A similar legal definition can be found in Spanish law, which refers to digital nomads as „international teleworkers". The only difference compared to the previous definition under Croatian law is that in Spain, digital nomads who engage in professional activities are authorized to work for companies located in Spain as long as that work does not exceed 20% of the total professional activity of the digital nomad.[27]

---

21 *Ibid*.

22 Nash, C. *et al*, *Digital Nomads Beyond the Buzzword: Defining Digital Nomadic Work and Use of Digital Technologies*, in: Chowdhury, G., *et al* (eds.), Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science, Vol. 10766, Springer, Cham, 2018, p. 213.

23 *Ibid.*

24 Bruurs, *op. cit.,* note 20, p. 3.

25 Art. 3 para. 1 subpara. 43 of the Crotian Immigration Act, Official Gazette No. 133/20, 114/22, 151/22.

26 *Ibid*.

27 Art. 74 bis of Law 28/2022 for the promotion of the ecosystem of emerging companies, Official Gazette No. 306.

3. CHARACTERIZATION OF THE INDIVIDUAL EMPLOYMENT CONTRACT IN EUROPEAN PRIVATE INTERNATIONAL LAW

The characterization of a specific legal relationship in private international law is of fundamental importance. Characterization requires that the facts characteristic of a particular legal relationship be categorized into one of the legal categories in order to correctly apply conflict of law rules and, consequently, the relevant substantive law.[28] Individual employment contracts fall under the protective categories of legal relationships for which specific rules on jurisdiction and the determination of applicable law are prescribed. The purpose of such rules is to protect employees as the weaker party in an asymmetric legal relationship, thus implementing the principle of the protection of the weaker party, as one of the fundamental principles of EU PIL for contractual relationships.[29] The fundamental rules of EU PIL concerning the protection of employees as the weaker party are contained in Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations[30] (hereinafter: Rome I Regulation) and 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[31] (hereinafter: Brussels I Recast Regulation). Although the Rome I and Brussels I Recast Regulations provide more favorable rules in favor of employees for determining applicable law and the competent court for individual employment contracts, these regulations do not include a specific legal definition of individual employment contracts, employees, or employers. The concept of an individual employment contract is of equivalent scope under the Rome I Regulation and the Brussels I Recast Regulation.[32]

The Court of Justice of the European Union (CJEU) has considered the concept of an individual employment contract in several PIL cases. As essential characteristics of an employment relationship, for the purposes of applying provisions on individual employment contracts, the CJEU has established the following:

---

28 Van Calster, G., *European Private International Law*, Hart Publishing, Oxford and Oregon, 2013, pp. 5-6.; *See also:* Sajko, K., *Međunarodno privatno pravo*, Narodne novine, Zagreb, 2009, p. 177.

29 Babić, D. A. and Zgrabljić Rotar, D., *Mjerodavno pravo za ugovorne odnose*, in: Josipović, T. (ed.), Privatno pravo Europske unije – Posebni dio, Narodne novine, Zagreb, 2022, p. 220.

30 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177.

31 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) [2012] OJ L 351.

32 Recital No. 7 of the Rome I Regulation.

1) the establishment of a long-term connection that partially places the worker within the organizational framework of the employer; and 2) the fact that one person, over a certain period of time, performs tasks for another person according to their instructions, in exchange for remuneration.[33] Identical characteristics of an employment relationship, in terms of the hierarchical relationship between the employer and the employee, the existence of subordination, and the presence of remuneration as consideration, have been established in other CJEU cases where the interpretation of secondary EU legislation was at issue.[34]

Furthermore, as previously mentioned, contracts entered into between platform workers/digital nomads and other contracting parties often contain a contractual clause that classifies service providers as self-employed individuals or independent contractors. This raises the question of whether such a contractual clause restrains a different classification of service providers under EU PIL. Such provisions do not prevent a different characterization of the legal relationship under EU law and consequently under EU PIL. This stance has been adopted by the CJEU, explaining that the formal classification of workers as self-employed individuals under national law does not preclude the classification of individuals as workers if their independence is solely conceptual.[35]

It is also worth noting that the characterization of a specific legal relationship as an employment relationship within the framework of EU PIL does not depend on the formal conclusion of a contract. The fact that the contracting parties have not formally entered into a contract does not affect the existence of an employment relationship under EU PIL, and therefore does not exclude the application of rules determining the applicable law and jurisdiction for individual employment contracts.[36] The impact of the absence of a formally concluded employment contract and the legal consequences thereof are assessed in accordance with the applicable substantive law to which conflict of law rules refer. Therefore, the concept of an individual employment contract in the context of PIL characterization of legal relationships involving platform workers/digital nomads should be interpreted autonomously in light of the case law of the CJEU, independent of national le-

---

33 Case 266/85 Hassan Shenavai v Klaus Kreischer [1987] ECLI:EU:C:1987:11, para. 16.; Case C-47/14 *Holterman Ferho Exploitatie BV and Others v F.L.F. Spies von Büllesheim* [2015] ECLI:EU:C:2015:574, para. 41.

34 See: Case C-413/13 *FNV Kunsten Informatie en Media v Staat der Nederlanden* [2014] ECLI:EU:C:2014:2411; Case C-692/19 *B v Yodel Delivery Network Ltd* [2020] ECLI:EU:C:2020:288.

35 Case C-256/01 *Debra Allonby v Accrington & Rossendale College* [2004] ECLI:EU:C:2004:18, para. 71. See also: Case C-413/13 *FNV Kunsten Informatie en Media v Staat der Nederlanden* [2014] ECLI:EU:C:2014:2411, para. 35.

36 Case C-603/17 *Peter Bosworth and Colin Hurley v Arcadia Petroleum Limited and Others* [2019] ECLI:EU:C:2019:310, para. 27.

gal concepts, to ensure uniform application of EU PIL sources and predictability across all EU Member States.[37]

In the context of atypical forms of work with digital characteristics, the significance of determining the legal status of platform workers or digital nomads will be influenced by the relationship of the other contracting party in terms of control over the performance of work and its results.[38] In the context of digital platforms, such control is commonly exercised through reviews, where the end-user of the service assesses their satisfaction with the provided service.[39] Based on these reviews, as well as other predetermined parameters, the digital platform, through algorithmic management, makes crucial decisions that impact the position of the platform workers and conditions of their work.[40] Therefore, the control of the employer over the employee in the digitalized world takes on an entirely new dimension compared to the traditional employer's supervision over the quality and efficiency of an employee's work. Although platforms, in order to minimize legal and fiscal obligations, consider themselves strictly as intermediaries, the control they exert over the work of platform workers through algorithmic management and rating systems can be seen as a modern substitute for traditional subordination, which is a fundamental characteristic of an employment relationship.[41]

In the *Yodel*[42] case, which originally does not fall within the scope of EU PIL, the CJEU established a series of criteria to make a negative distinction between the concept of a self-employed person and the concept of a worker. The underlying assumptions for determining a genuinely self-employed person are that the person's independence is not fictitious, and there is no relationship of subordination.[43] If these assumptions are met, then a self-employed person cannot be classified as a worker, provided that the person is also discretionarily authorized: 1) to use subcontractors or substitutes to perform the service which he/she has undertaken to provide; 2) to accept or not accept the various tasks offered by his/her putative employer, or unilaterally set the maximum number of those tasks; 3) to provide his/her services to any third party, including direct competitors of the putative

37 Van Calster, *op. cit.*, note 1, p. 475.

38 De Stefano, V., *Introduction: Crowdsourcing, the Gig-Economy and the Law*, Comparative Labor Law & Policy Journal, Vol. 37, No. 3, 2016, p. 4.

39 *Ibid*.

40 Bjelinski Radić, I., *Kritička promišljanja o prijedlogu Direktive o poboljšanju radnih uvjeta platformskih radnika*, Zbornik Pravnog fakulteta u Zagrebu, Vol.72, No. 6, 2022, p. 1472.

41 Naumowicz, K., *Some remarks to the legal status of platform workers in the light of the latest European jurisprudence*, Studia Z Zakresu Prawa Pracy I Polityki Społecznej, Vol. 28, No. 3, 2021, p. 179.

42 Case C-692/19 *B v Yodel Delivery Network Ltd* [2020] ECLI:EU:C:2020:288.

43 *Ibid.,* para. 45.

employer; and 4) to fix his/her own hours of 'work' within certain parameters and to tailor his/her time to suit his/her personal convenience rather than solely the interests of the putative employer.[44]

Considering the disparity of legal relationships with the performance of work with digital features, the characterizaton of legal relations within the framework of EU PIL might be facilitated in the future by the Directive of the European parliament and of the Council on improving working conditions in platform work (hereinafter: Platform Work Directive)[45]. The mentioned Directive is the result of the European Commission's recognition of the complexity of correctly determining the labour status of platform workers, as well as the phenomenon of false self-employment.[46] Consequently, an incorrect labour classification of the legal relationship, where one of the parties is a person working through a platform, can have consequences such as depriving that person of labour protections and other rights within the social security system.[47] The general aim of the Directive on platform work is to improve working conditions and social rights for individuals working through "digital labour platforms"[48].[49] This overarching goal should be achieved through the realization of the following specific objectives: 1) ensuring the appropriate employment status for individuals working through platforms based on their actual relationship with the platform; 2) ensuring fairness, transparency, and accountability in algorithmic management by platforms; and 3) increasing transparency, traceability, and awareness of developments in platform work while enhancing the enforcement of rules for all individuals, including those working cross-border through digital labour platforms.[50]

Ratione materiae, the Platform Work Directive establishes minimum rights that apply to individuals working in the EU through platforms, including those with employment contracts or considered to have employment contracts, or those in an employment relationship under national law, collective agreements, or practices

---

44 *Ibid.*

45 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work [2021] COM/2021/762 final.

46 Bjelinski Radić, *op. cit.*, note 40, p. 1472.

47 *Ibid.*

48 Pursuant to Art. 2(1)(1) of the Platform Work Directive, a digital labour platform is defined as „any natural or legal person providing a commercial service which meets all of the following requirements: (a) it is provided, at least in part, at a distance through electronic means, such as a website or a mobile application; (b) it is provided at the request of a recipient of the service; (c) it involves, as a necessary and essential component, the organisation of work performed by individuals, irrespective of whether that work is performed online or in a certain location".

49 Platform Work Directive., p. 3.

50 *Ibid.*

applicable in the Member States, taking into account the CJEU's jurisprudence.[51] *Ratione persone*, the Platform Work Directive applies to all individuals performing platform work, regardless of how their relationship is classified between the contracting parties.[52] In terms of territorial scope, the Platform Work Directive applies to digital labour platforms that organize work through platforms performed in the EU, irrespective of the location of their registered office and the law otherwise applicable.[53]

In the context of the discussion on the characterization of the legal relationship, it is important to note that the Platform Work Directive introduces a legal presumption of the existence of an employment relationship between the person working through a platform and the digital labour platform that supervises the work.[54] To achieve this presumption, the Platform Work Directive sets out a series of indicators that establish the platform's control over the person working through the platform. In defining these indicators, the European Commission was clearly inspired by the CJEU's decision in the *Yodel*[55] case.[56]

According to the Platform Work Directive, it is considered that there is control by the digital labour platform over the person working through the platform if at least two of the following conditions are met:

a) *„effectively determining, or setting upper limits for the level of remuneration;*

b) requiring the person performing platform work to respect specific binding rules with regard to appearance, conduct towards the recipient of the service or performance of the work;

c) supervising the performance of work or verifying the quality of the results of the work including by electronic means;

d) effectively restricting the freedom, including through sanctions, to organise one's work, in particular the discretion to choose one's working hours or periods of absence, to accept or to refuse tasks or to use subcontractors or substitutes;

e) effectively restricting the possibility to build a client base or to perform work for any third party".[57]

---

51 Art. 1(2) of the Platform Work Directive.

52 Ratti, L., *A Long Road Towards the Regulation of Platform Work in the EU*, in: Boto, J. M. M. and Brameshuber, E. (eds), Collective Bargaining and the Gig Economy, Hart Publishing, Oxford, 2022, p. 50.

53 Art. 1(3) of the Platform Work Directive.

54 *Ibid*., Art. 4(1).

55 See *supra* notes no. 41-43.

56 Bjelinski Radić, *op. cit.*, note 40, p. 1480.

57 Art. 4(2) of the Platform Work Directive.

The legal presumption of the existence of an employment relationship is rebuttable, and the possibility of rebuttal can be exercised by both, the digital labour platform and the person working through the platform, in judicial and/or administrative proceedings.[58] In case the presumption of an employment relationship is challenged by the digital labour platform, it is worth noting that, in line with the principle *in favorem laboratoris*, the burden of proof lies with the digital labour platform.[59]

When the Platform Work Directive comes into effect, it will become an integral part of European substantive law and will consequently be implemented into the national legislation of EU Member States. Therefore, the question arises as to whether the conditions for establishing the legal presumption can serve as indicators for characterizing contractual relationships as individual employment contracts in which the parties are platform workers, as well as digital nomads if they work through a platform, in the context of EU PIL? The answer to this question should be affirmative. Indeed, in several cases, the CJEU has interpreted the term „employee" in the context of EU PIL in light of other Union legislative acts. In the *Holterman* case, the CJEU took the position that when determining the concept of an employee in the context of EU PIL, one should take into account the features of the term "worker" in accordance with primary and secondary EU law, referring to certain directives in the field of European labour law.[60]

Furthermore, in the proposal for the Platform Work Directive, it is stated that it applies to digital labour platforms that organize work through platforms performed in the Union, regardless of the place of business establishment of the platform and regardless of the law that would otherwise apply.[61] From this, it is evident that the exclusive criterion for the application of the provisions of the Platform Work Directive is that the work is carried out within the EU. Therefore, when characterizing legal relationships under EU PIL that involve platform work, a systematic interpretation of EU law should be applied, starting from the mentioned presumption, and at the conflict of laws level, characterize the legal relationship as an employment relationship. Additionally, the Platform Work Directive emphasizes that the legal presumption of the existence of an employment relationship applies in all relevant administrative and legal proceedings, and competent authorities are authorized to rely on such a legal presumption.[62]

---

58 *Ibid.,* Art. 5(1).

59 *Ibid*., Art. 5(2).

60 Case C-47/14 *Holterman Ferho Exploitatie BV and Others v F.L.F. Spies von Büllesheim* [2015] ECLI:EU:C:2015:574, paras. 41-42.

61 Art. 1(3) of the Platform Work Directive.

62 Art. 4(1) of the Platform Work Directive.

In conclusion, an additional reason for applying the indicators of the existence of an employment relationship from the Platform Work Directive in terms of conflict of law characterization can be argued using the teleological method of interpreting EU law. The Treaty on the Functioning of the European Union, as one of its objectives in the field of social policy, defines the improvement of working conditions for workers.[63] The Platform Work Directive, at the substantive level, contributes to the protection of workers in the context of modern forms of work through digital labour platforms by introducing a presumption of the existence of an employment relationship, thereby achieving protection for workers as the weaker contracting party. Therefore, for consistency in the interpretation of EU law and to achieve the objectives of social policy, special conflict-of-law rules for individual employment contracts should also be applied, and the indicators from the Platform Work Directive should be considered in characterizing the employment relationships of platform workers.

4. APPLICABLE LAW

As previously mentioned, the Rome I Regulation provides special conflict of law rules for individual employment contracts with the aim of protecting workers as the weaker party in the contract. The reason for having special conflict of law rules for individual employment contracts lies in the vulnerability of employees due to their specific position in relation to the employer. In general contract law, parties are considered equal, which is expressed through the principle of coordination. On the other hand, in employment relationships, the principle of subordination comes into play. Under EU PIL, an employee is considered to be in a legally vulnerable position due to information asymmetry regarding the content of the applicable law.[64] Additionally, the vulnerability of employees can be attributed to economic and social subordination. Most employees depend on their work as the primary source of income, and employment contributes significantly to an individual's personal and societal fulfillment.[65]

The concept of "applicable law" under the Rome I Regulation refers to any law indicated by the conflict of law rule, regardless of whether it is the law of an EU Member State.[66] Therefore, it is possible in certain legal situations for the appli-

---

63 Art. 151(1) of the Treaty on the Functioning of the European Union [2012] OJ C 326.

64 Rühl, G., *The Protection of Weaker Parties in the Private International Law of the European Union: A Portrait of Inconsistency and Conceptual Truancy*, Journal of Private International Law, Vol.10, No. 3, 2014, pp. 343-344.

65 *Ibid.*, pp. 344-355.

66 Art. 2 of the Rome I Regulation.

cable law to be the law of a third country (non-EU). This is crucial in the context of platform workers and digital nomads, given the mobility that these atypical forms of work offer. Such a broad, *erga omnes* reach of the Rome I Regulation in private international law is referred to as the principle of universal application.[67]

In determining the applicable law for individual employment contracts, it is important to distinguish between subjective and objective applicable law. Subjective applicable law for individual employment contracts is the law chosen by the parties (*lex autonomiae*).[68] In cases where there is no party choice of applicable law or such a choice is invalid, objective applicable law is applied. Also, objectively applicable law is applied in cases where there is a party's choice of applicable law, but this chosen law provides the employee with a lower level of protection compared to the mandatory provisions of objectively applicable law.[69] When determining the objective applicable law, there are several steps. First and foremost, the objective applicable law is the law of the country where, or from which, the employee habitually carries out his work based on the contract (*lex loci laboris*).[70] If it is impossible to determine such a location, the objective applicable law becomes the law of the country of the engaging business.[71] However, regardless of these two previously mentioned objective connecting factors, the Rome I Regulation for individual employment contracts also includes an escape clause. This means that if, from all the circumstances of the case, it is clear that the individual employment contract is closely connected with a country other than the country where the employee habitually carries out his/her work or the country where the place of business is located, then the law of that other country shall apply.[72]

Before discussing the previously mentioned rules for determining the applicable law in the context of platform workers and digital nomads, it is important to note that there are contracts that will not be characterized as individual employment contracts within the meaning of EU PIL. For such general contracts, the general rules for determining the applicable law under the Rome I Regulation apply. This means that in the context of platform workers and digital nomads, legal relationships will be assessed according to the chosen law, and subsidiarily, according to the law of the country where the service provider has their habitual residence.[73]

---

67 Sajko, *op. cit.*, note 28, p. 61.; *See also:* Art. 2 of the Rome I Regulation.

68 Art. 8(1) of the Rome I Regulation.

69 See *infra* note 78.

70 Rome I Regulation, Art. 8(2).

71 *Ibid*., Art. 8(3).

72 *Ibid.*, Art. 8(4).

73 Cherry, M. A., *A Global System of Work, A Global System of Regulation?: Crowdwork and Conflicts of Law*, Tulane Law Review, Vol. 94, 2019, p. 36.

If the legal relationship in question cannot be characterized as a service contract, then it falls under the law of the country where the party who performs the characteristic performance has their habitual residence.[74] Additionally, in this case, the escape clause is present.[75]

4.1. Choice of law (*lex autonomiae*)

Considering that party autonomy is a fundamental principle in contemporary private law, the European legislator, through the Rome I Regulation, allows the parties to an individual employment contract to choose the law that will be applicable to their legal relationship.[76] However, such a choice of law by the parties is not unlimited.[77] In order to protect employees as the weaker party, the Rome I Regulation prescribes that the parties' choice of law cannot deprive the employee of the protection provided by mandatory provisions of the objectively applicable law that would have been applicable if the parties had not made a choice of law.[78]

In the context of platform workers who exclusively work in an online environment and digital nomads, choosing the applicable law would be the most desirable solution due to potential difficulties in localizing the place of work or changes in the work location. Such a choice of applicable law introduces predictability and stability into the legal relationship between the platform worker or digital nomad and the employer.[79] However, regardless of the chosen law, even if the initiative came from the employer, platform workers and digital nomads will always be guaranteed the protection of mandatory provisions of the objectively applicable law.[80]

In this regard, the court must first determine the law that would have been applicable if no choice of law had been made and determine the mandatory provisions from that law.[81] Then, in the next step, the court compares the level of protection that the employee enjoys based on those provisions with the level of protection

---

74 *Ibid*.

75 Art. 4(3)(4) of the Rome I Regulation.

76 Kunda, I., *Međunarodnoprivatnopravni odnosi*, in: Mišćenić, E. (ed.), Europsko privatno pravo. Posebni dio., Školska knjiga, Zagreb, 2021, pp. 523-524.

77 Staudinger, A., *Article 8: Individual employment contracts*, in: Ferrari, F. (ed), Rome I Regulation, Pocket Commentary, Sellier European Law Publishers, Munich, 2015, p. 297.

78 Art. 8(1) of the Rome I Regulation.

79 Bruurs, *op. cit.*, note 20, p. 4.

80 Art. 8 of the Rome I Regulation.

81 Joined Cases C-152/20 and C-218/20 *DG and EH v SC Gruber Logistics SRL and Sindicatul Lucrătorilor din Transporturi v SC Samidani Trans SRL* [2021] ECLI:EU:C:2021:600, para. 27.

provided by the chosen law.[82] If the chosen law provides better protection, it is applied.[83] It is important to note that the objectively applicable law must meet two prerequisites to be applied despite the parties' choice of law. First, such provisions must be mandatory in character, and second, they must provide the employee with a higher level of protection than the chosen applicable law.[84] Therefore, mandatory provisions of the objectively applicable law will not be applied if they do not provide the employee with greater protection.[85] In the opposite situation, if the mandatory provisions of the objectively applicable law provide the employee with greater protection, these provisions are primarily applied, followed by other provisions of the chosen law. In this case, the phenomenon known as „law mix" occurs.[86]

Finally, it is important to consider the question of the validity of the choice of law when the applicable law, which will be a common occurrence, is proposed by the employer to the platform worker or digital nomad in the form of a standardized contract. Such a choice of applicable law is not problematic as long as the employee has freely agreed to such a contractual clause. CJEU has taken the position in the case of *SC Grbuer Logistics* that the Rome I Regulation does not prohibit the use of standard contractual clauses that the employer has previously drafted, and that the freedom to choose the law can be exercised by agreeing to such a contractual clause. It is not inherently problematic that the employer has drafted and included such a clause in the contract.[87]

4.2. Habitual place of work (*lex loci laboris*)

As previously mentioned, the objectively applicable law for individual employment contracts is the law of the country where, or from which, the employee habitually performs his work.[88] This connecting factor is primarily applied when the parties have not made a choice of law or when the choice of law is invalid. It is also applied when the mandatory provisions of the law of the country where

---

82 *Ibid*.

83 *Ibid*.

84 Sinander, E., *The Role of Foreseeability in Private International Employment Law*, Nordic Journal of Labour Law, Vol. 1, No. 1, 2023, p. 9.

85 *Ibid*.

86 Rühl, *op. cit.*, note 64, pp. 352-353.

87 Joined Cases C-152/20 and C-218/20 *DG and EH v SC Gruber Logistics SRL and Sindicatul Lucrătorilor din Transporturi v SC Samidani Trans SRL*, *op. cit.*, note 81, para. 40.

88 Art. 8(2) of the Rome I Regulation.

the employee habitually works provide a higher level of protection for the worker compared to the chosen applicable law. [89]

Determining the place of work should not present a significant obstacle in the context of platform workers who perform work at a specific physical location (on-demand; offline), such as delivery jobs, transportation, and household work. However, the situation is somewhat more complex in the context of platform workers whose work is exclusively carried out in an online environment, as well as digital nomads. In these cases, the results of the work are delivered solely in a digital environment (digital platform, cloud, email, etc.), without the need for physical work at a specific location. Since the work of such employees typically involves data entry, the applicable law should be the law of the country where the worker habitually performs data entry because that is where the essential content of the work is carried out. [90] However, in relation to platform workers who exclusively perform their work online, the habitual place of work as a connecting factor might be inappropriate due to the facilitation of social dumping. Specifically, employers from one country may be incentivized to hire platform workers from other countries with lower labour costs or lower levels of employee protection, who would perform online platform work in those countries. In such a scenario, the law of the habitual place of work would constitute the objectively applicable law. This would run contrary to the Rome I Regulation, which, among other things, adopts an anti-dumping approach in determining the applicable law for individual employment contracts.[91]

Furthermore, determining the place of work, in the context of platform workers and digital nomads, becomes more complex when there is a change in the place of work during the duration of the employment contract with the same employer. Especially in the context of the mobility of digital nomads, it is common for them to change the countries from which they work while the employment contract is in effect. In such cases, a change in the place of work as a connecting factor for determining the applicable law occurs. Consequently, such a change in the place of work raises the question of which law is applicable to the specific legal relationship. In terms of private international law, this is referred to as „*conflits mobiles*". [92] In the case of individual employment contracts, such a change is possible be-

---

89 See *supra* chapter 4.1.

90 Staudinger, *op. cit.*, note 77, p. 303.

91 Bruurs, S., *Cross-border telework in light of the Rome I-Regulation and the Posting of Workers Directive*, European Labour Law Journal, Vol. 0, No. 0, 2023, p. 20.

92 The rule of conflict of laws remains unchanged, but during the duration of a certain legal relationship, the facts on which the connecting factor is based change, which may result in a change in the applicable law. Only possible with variable connection factors. See: Sajko, *op. cit.*, note 28, p. 248-249.

cause the habitual place of work is a changeable connecting factor. On the other hand, habitual residence as a general connecting factor in the law applicable to contracts is also a changeable connecting factor, but with a significant difference regarding the decisive moment for determining the habitual residence. Namely, it is certainly possible to establish a new habitual residence during the duration of a certain long-term legal relationship, but the decisive moment for determining the habitual residence of the contracting party is temporally fixed to the moment of contract conclusion.[93] Therefore, any subsequent changes in habitual residence are irrelevant. On the other hand, for the habitual place of work, as a connecting factor for the objective applicable law in individual employment contracts, a similar provision does not exist in the Rome I Regulation. It is, therefore, unquestionable that during the duration of a certain employment contract, it is possible to change the habitual places of work, which poses a challenge to courts in determining the applicable law. In the case of platform workers and digital nomads, the habitual place of work, if possible, will be localized based on the main center of actual performance.[94] Accordingly, the habitual place of work will be in the country where the platform worker or digital nomad actually performs the essential content of their work activities.[95] This is further emphasized in the *Koelzsch* case, where the CJEU clarified that the habitual place of work should be considered the country where the employee fulfills the greater part of their obligations towards the employer.[96] However, given the pronounced mobility of digital nomads, as well as platform workers who exclusively work in an online environment, assessing from which country the employee has performed the greater part of their obligations could be challenging. In these forms of work, the achievement of the end result by the employee is usually crucial, while the hours worked are not as relevant as in conventional employment relationships.

The purpose of the „habitual place of work" as a connecting factor is to implement the principle *in favorem laboratoris* because it is believed to be in the employee's interest.[97] However, in the case of non-conventional (digitized) forms of work, the question arises of whether the application of this connecting factor genuinely serves the interests of platform workers and digital nomads. In the case of static platform workers who do not change their country of work, the contribution to

93 Art. 19(3) of the Rome I Regulation.

94 Staudinger, *op. cit.*, note 77, p. 303.

95 Mota, C. E. and Moreno, G. P., *Article 21* in: Magnus, U. and Mankowski, P. (eds) European Commentaries on Private International Law, ECPIL, Brussels Ibis Regulation, Verlag Dr. Otto Schmidt, Köln, 2016, p. 547.

96 Case C-29/10 *Heiko Koelzsch v État du Grand Duchy of Luxemburg* [2011] ECLI:EU:C:2011:151, para. 50.

97 Sinander, *op. cit.*, note 84, p. 14.

the *in favorem laboratoris* principle is undisputed. However, for mobile platform workers and digital nomads, it is questionable how closely the law of a country where they temporarily reside for only a few months, and then move to another country for a few months, relates to their actual interests. This leads to the conclusion that the „habitual place of work" as a connecting factor is not the most appropriate solution when determining the applicable law for employment relationships in which the contracting parties are digital nomads and mobile platform workers. The inadequacy lies in the fact that in such cases, the purpose of special conflict rules for employment relationships is not achieved, and consequently, the law that is closest and most familiar to the contracting parties is not applied.[98]

4.3. Place of business

In cases where it is impossible to determine the habitual place of work of an employee, the subsidiary applicable law is that of the country where the place of business through which the employee is engaged is located.[99] In contrast to the broad interpretation of the habitual place of work, the place of business as a connecting factor is applied exceptionally, with a narrow interpretation.[100] This rule of conflict of laws was primarily designed for mobile workers, such as international transport workers.[101] It is worth noting that this rule of conflict of laws applies to all employment relationships in which the employee does not work from a single permanent location or when the employee has multiple permanent habitual places of work of equal importance located in different countries.[102] Specifically, the interpretation of this connecting factor was provided by the CJEU in the *Voogsgeerd* case.[103] The Court indicated that the term "engaged" refers exclusively to the conclusion of an employment contract. If a contract is not concluded and there exists a *de facto* employment relationship, then the focus shifts to the establishment of the employment relationship.[104] Relevant circumstances related to the process of concluding an employment contract, or the establishment of an employment relationship, include the place of business that published the job advertisement and the place

---

98 Josipović, T., *Privatno pravo Europske unije – Opći dio*, Narodne novine, Zagreb, 2020, p. 103.

99 Art. 8(3) of the Rome I Regulation.

100 Merrett, L., *Jurisdiction over Individual Contracts of Employment*, in: Dickinson, A. and Lein, E. (eds), The Brussels I Regulation Recast, Oxford University Press, Oxford, 2015, p. 250.

101 Pretelli, I., *A focus on platform users as weaker parties*, in: Bonomi, A. and Romano, G. P. (eds), Yearbook of Private International Law – 2020/2021, Vol. 22, Verlag Dr. Otto Schmidt, Köln, 2021, p. 221.

102 Grušić, U., *The European Private International Law of Employment*, Cambridge University Press, Cambridge, 2015, p. 167.

103 Case C-384/10 *Jan Voogsgeerd v Navimer SA* [2011] ECLI:EU:C:2011:842.

104 *Ibid.*, para. 46.

of business that conducted the selection process for potential employees.[105] Given that only circumstances related to the process of concluding an employment contract are considered, other circumstances related to the actual performance of work are entirely irrelevant.[106]

Some authors argue that the place of business through which an employee is engaged could be the most appropriate connecting factor for determining the applicable law in the context of platform workers, particularly to prevent social dumping.[107] This argument may be acceptable in situations where the place of business is within the EU because it provides a high level of labour law protection to employees compared to, for example, the laws of third countries. Furthermore, it ensures fair market competition among employers within the EU because they are obliged to respect comparable labour law and fiscal obligations inherent in the rights of EU Member States arising from the existence of an employment relationship. However, there could hypothetically be a different situation. This would be the case when the place of business is located in a third country, and the habitual place of work cannot be specifically determined. In such a situation, there is a risk of applying the substantive law of the third country, which may provide a lower level of labour law protection to the employee compared to EU states, or even classify the employment relationship with the employee under the law of the third country as a non-employment relationship. Additionally, an argument against the appropriateness of this connecting factor can be seen in the process of concluding contracts or in the establishment of a *de facto* employment relationship. Digital technologies enable fast and straightforward communication and contract formation that does not require the physical presence of both contracting parties, such as in the employer's business premises. Therefore, there is a risk that in such a situation, the employee is not even aware of the country where the place of business through which they are engaged is located, or which law is applicable.

In conclusion, the place of business through which an employee is engaged would not be the most appropriate solution for determining the applicable law for platform workers and digital nomads. The reason for this, as evident from the discussion above, lies in the fact that it does not establish a specific connection between a particular employment relationship and the law of a specific country, and therefore, it does not establish a clear link between the employee and the law of a particular country.[108] Given the lack of a concrete connection between the employment

105 *Ibid.*, para. 50.

106 Staudinger, *op. cit.,* note 77, p. 314.

107 Pretelli, *op. cit.*, note 101, p. 221.

108 Bruurs, *op. cit.,* note 20, p. 5.

relationship and the applicable law based on the place of business, the application of this connecting factor does not serve the purpose of private international law, which aims to apply the law of the country with which the legal relationship has the closest connection. This approach could lead to legal uncertainty and unpredictability in the legal relationship for the employee, which does not contribute to achieving the goals of protecting employees.[109]

4.4. Escape clause

An escape clause allows the court to apply the law of another country, which the court considers to have a closer connection to the specific legal relationship, instead of the law indicated by the conflict of laws rules.[110] Comparing the connecting factor of the habitual place of work and the escape clause, what they have in common is that both are based on the principle of closest connection, which is a fundamental principle of private international law. However, in the case of the habitual place of work, the closest connection is territorially specified, whereas in the case of the escape clause, the court has the authority to, taking into account all the circumstances of the case, apply the law that is closest related to the particular legal relationship and thereby correct the reference to the law of the country that the legislator presumed to be the closest by establishing a link within the conflict of laws rules.[111]

In the context of platform workers and digital nomads, given their high mobility, the escape clause could serve as the most suitable solution for determining the applicable law. This is especially relevant for digital nomads and platform workers whose work is carried out exclusively in a virtual environment, and who may change the country from which they work two or more times during the duration of a single employment contract with the same employer, making the territorial specification of the place of work challenging. For instance, in the *Schlecker* case, the CJEU established a series of indicators that can be used to determine whether a particular employment relationship has a closer connection with another country, different from the one indicated by the aforementioned objective criteria. Relevant indicators include the country where the employee pays taxes, as well as the country where the employee participates in the social security and healthcare system. Additionally, the overall circumstances of the case should be considered,

---

109 Grušić, U., *Should the Connecting Factor of the 'Engaging Place of Business' be Abolished in European Private International Law?*, International & Comparative Law Quarterly, Vol. 62, No. 1, 2013, p. 173.

110 Župan, M., *Načelo najbliže veze u hrvatskom i europskom međunarodnom privatnom ugovornom pravu*, Pravni fakultet u Rijeci, Rijeka, 2006, p. 27.

111 Kunda, *op. cit.*, note 76, pp. 509-510 and pp. 519-521.

especially parameters for determining salary or other working conditions.[112] Apart from the indicators mentioned earlier in line with CJEU's case law, other factors such as the worker's citizenship and residence, the method of salary calculation, and the language of the contract and currency of payment could also be considered, albeit exceptionally, in cases where they are atypical.[113]

However, the escape clause is applied restrictively in EU PIL, only in cases where the previously applicable objective connecting factors do not contribute to the principle of the closest connection for a specific legal relationship.[114] The restrictive application of the escape clause means that the court cannot automatically exclude the habitual place of work and apply the escape clause, even if all other circumstances, except for the place of work, point to the law of another country.[115] In other words, courts are obligated to consider all circumstances of the legal relationship as a whole and determine which circumstance is the most significant.[116]

Despite the general restrictiveness, the application of the escape clause concerning individual employment contracts is indeed more flexible in comparison to other escape clauses within the Rome I Regulation. The provision regarding the escape clause in Article 8 of the Rome I Regulation does not include the "manifestly" requirement, as is the case with the escape clause in Article 4(3) of the Rome I Regulation or escape clauses within provisions pertaining to carriage contracts or insurance contracts.[117] Consequently, in the context of individual employment contracts for platform workers or digital nomads, the court would have greater latitude in "bypassing" the prior connecting factors of objectively applicable law if it is evident from all circumstances of the case that the employment contract is more closely connected with the law of another country, without the need to satisfy the manifestly criterion, which represents a more stringent requirement in other escape clauses. Such a designed escape clause pertaining to individual employment contracts significantly contributes to the flexibility in determining the applicable law for the employment relationships of digital nomads or platform workers. Certainly, it is important to emphasize that the absence of the "manifestly" criterion by no means implies that the court is not obligated to provide reasoning based on which indicators it has chosen to apply the law of another country as the appli-

112 Case C-64/12 *Anton Schlecker v Melitta Josefa Boedeker* [2013] ECLI:EU:C:2013:551, para. 41.

113 Bruurs, *op. cit.*, note 20, p. 5.

114 Kunda, *op. cit.*, note 76, pp. 519-520.

115 Case C-64/12 *Anton Schlecker v Melitta Josefa Boedeker*, *op. cit.,* note 112, para. 40.

116 *Ibid.,* para. 41.

117 Arts. 5(3) and 7(2) of the Rome I Regulation.

cable law, rather than the law of the country indicated by the previously applicable objective connecting factors.

To support the argument that the escape clause is the most suitable tool for determining the applicable law in the case of digital nomads, consider a hypothetical example: An employee with habitual residence in an EU Member State works as a digital nomad in several third countries, providing remote work for an EU-based employer. It is difficult to believe that any of the third countries from which the nomad works during a certain period could genuinely represent the seat of the specific employment relationship, and thus, the habitual place of work in terms of territorial specification of the principle of the closest connection. Therefore, as previously mentioned, in the case of highly mobile employees like digital nomads, the escape clause would be the most optimal way to determine the applicable law by taking into account a series of indicators that justify the application of the law of a specific country as the applicable law.[118]

4.5. Overriding mandatory provisions

According to the Rome I Regulation, overriding mandatory provisions are those considered essential for safeguarding a state's public interests, such as its political, social, or economic structure, irrespective of the law that would otherwise be applicable to a contract.[119] These mandatory provisions can be recognized as binding within the jurisdiction where the proceedings are conducted (*lex fori*), but also within the jurisdiction where the obligations arising from the contract were intended to be performed or have already been performed.[120] In general, the characteristic of overriding mandatory provisions is that such binding rules are directly applicable to any situation falling within their scope, regardless of its international nature, and they cannot be circumvented by the choice of law rules.[121] However, with respect to individual employment contracts, the application of overriding mandatory provisions is somewhat limited. This pertains to situations where mandatory provisions of the objective applicable law provide the employee with a higher level of protection compared to overriding mandatory provisions of the forum's law, which also aim to protect employees. In such cases, priority should still be given to the mandatory provisions of the objectively applicable law.[122]

---

118 See *supra* notes 112 and 113.

119 Art. 9(1) of the Rome I Regulation.

120 Art. 9 (2)(3) of the Rome I Regulation.

121 Babić; Zgrabljić Rotar, *op. cit.*, note 29, p. 232. See also Van Calster, *op. cit.*, note 1, p. 471.

122 Campo Comba, M., *The Law Applicable to Cross-border Contracts involving Weaker Parties in EU Private International Law*, Springer, Cham, 2020, pp. 161-162.

In the context of platform workers and digital nomads, there is a possibility that work may be carried out in a third country (non-EU), while the employer is located in a Member State of the EU. According to the rules of international jurisdiction for individual employment contracts, employees are authorized, *inter alia*, to file a lawsuit against the employer before the court of the Member State where the employer has its domicile. However, they can also file a lawsuit before the court where the branch that employed the worker is located or was located, in cases where the employee does not regularly perform or did not perform his work in the same country.[123] In both of these situations, the competent court of the Member State will apply the rules for determining the applicable law from the Rome I Regulation, and consequently, potentially the substantive law of the third country as the objectively applicable law. The fact that the court of the Member State, according to EU PIL, characterizes a certain contract as an individual employment contract does not necessarily mean that the same characterization will be applied in terms of the applicable substantive law of the third country referred to by the conflict rule. Therefore, it is possible that, according to the substantive law of the third country, the platform worker or digital nomad may be classified as a self-employed individual, or an independent contractor. In such a case, the specific legal relationship will be assessed according to contract law, rather than labour law.

From the above, it raises the question of whether the rebuttable presumption regarding the existence of an employment relationship under the Platform Work Directive, when it comes into effect and is transposed into the national laws of Member States, can be considered a overriding mandatory provision of EU Member State law before whose court the proceedings are taking place. Providing a definitive answer to this question is difficult, as it depends on the specific factual circumstances of each individual case. The overriding nature arises from the text of the Platform Work Directive itself. Article 1(3) of the Platform Work Directive stipulates that *„This Directive applies to digital labour platforms organising platform work performed in the Union, irrespective of their place of establishment and irrespective of the law otherwise applicable"*.[124] From this, it follows that the overriding nature of the provisions of the Platform Work Directive is limited *ratione territorii*, as it is a necessary prerequisite that platform work is carried out within the territory of the Union. On the other hand, in situations where a platform worker or digital nomad performs work through a platform from a third country for an employer in the Union, such a situation falls outside the scope of the Platform Work Directive. Therefore, in such situations, the provisions of the Directive, including

[123] Art. 21(a)(b) of the Brussels I Recast Regulation.

[124] Art. 1(3) of the Platform Work Directive.

the presumption of the existence of an employment relationship, would not initially be considered overriding mandatory provisions. However, this contradicts the proclaimed goals of the Platform Work Directive. As the desired effect of the Platform Work Directive, in addition to improving the transparency of digital platforms' work, the Commission states that not only platform workers but also Member States will benefit directly in terms of increased tax collection and social security contributions. [125] [126]

Indeed, by denying the overriding nature of the Platform Work Directive in situations where platform work is conducted from third countries for an employer in the Union, it would directly benefit employers within the Union to engage workers from third countries with lower levels of protection or individuals with habitual residence within the Union who have chosen to live a nomadic life in various third countries. This would negatively impact the labour market in EU Member States, and such employers would represent unfair competition to employers whose platform workers perform work within the Union. This would also result in labour and fiscal obligations for the employer, thereby increasing business costs.

In the case-law of courts in Member States, there is a different approach to interpreting the purpose of overriding mandatory provisions. German practice and scholars believe that overriding mandatory provisions should at least partially serve to protect the state's interest, while French practice considers that overriding mandatory provisions can also serve to protect individual interests, such as employees.[127] Therefore, it would be reasonable to recognize the effect of the provisions of the Platform Work Directive, when transposed into the national laws of Member States, as overriding mandatory provisions, even in cases where platform work is performed outside the Union. Moreover, Member States are authorized, within the margin of appreciation, to give certain rules the significance of overriding mandatory provisions, if such a rule is based on EU law but exceeds the level of protection required by EU law.[128] Such an application would achieve dual protection of interests, including public interests related to equal market competition and the preservation of labour costs, as well as private interests of employees in terms of better labour protection and working conditions.

---

125 Platform Work Directive, p. 14.

126 The European Commission estimates that Member States could benefit from an increase in taxes and contributions for social protection in the amount of up to EUR 4 billion per year. See *ibid.*, note 125.

127 Van Bochove, L. M., *Overriding Mandatory Rules as a Vehicle for Weaker Party Protection in European Private International Law*, Erasmus Law Review, No. 3, 2014, pp. 149-150.

128 *Ibid.*, p. 149.

5. CONCLUDING REMARKS

The development of digital technologies is bringing about changes in various aspects of social life, and the field of work is no exception. The need for additional sources of income and the desire for flexibility in work compared to conventional forms of employment have led to the emergence of digital nomads and platform workers. Given the increasing prevalence of these phenomena and the growing mobility in work facilitated by digital technologies, it is expected that in the future, disputes with international elements involving digital nomads and platform workers as parties will become more common. This poses challenges for EU PIL. The first challenge is the correct characterization of the legal relationship involving platform workers or digital nomads in terms of conflict of laws. This is of paramount importance due to the existence of special rules for determining the applicable law for individual employment contracts, with the aim of protecting employees as the weaker contracting party. Additionally, there is the issue of concealed self-employment aimed at avoiding fiscal and labour regulations. In the conflict of law characterization, in light of the CJEU case-law, only the factual characteristics of a particular relationship should be considered, regardless of the characterization of the legal relationship by the contracting parties. Furthermore, in the context of EU PIL, the dilemma about the characterization of atypical, digital forms of work will be facilitated by the Platform Work Directive, which introduces a presumption of an employment relationship along with several indicators designed specifically for platform work. These indicators will undoubtedly be a useful tool for characterizing the legal relationships of digital nomads who do not necessarily perform work through a specific digital platform but whose work involves other digital elements.

Regarding the determination of the applicable law and for the sake of legal certainty for both contracting parties, the most acceptable solution is for the platform worker or digital nomad and the employer to autonomously choose the applicable law for their legal relationship. In the absence of a choice of law, the legal framework of the Rome I Regulation provides an adequate answer for determining the objectively applicable law. In the case of platform workers who work offline, meaning at a specific physical location, determining the objectively applicable law through the connecting factor of the habitual place of work should not pose significant difficulties. However, for mobile digital nomads and platform workers who work exclusively in an online environment, the escape clause would represent the optimal solution for determining the applicable law. By applying the escape clause, in comparison to other connecting factors for individual employment contracts, the principle of the closest connection is best realized as it contributes to the application of the law that is closest and most familiar to the contracting parties, thereby ensuring the protection of employees as the weaker contracting party.

REFERENCES

BOOKS AND ARTICLES

1. Aloisi, A., *Platform Work in the EU: Lessons learned, legal developments and challenges ahead,* European Commission, Brussels, 2020
2. Babić, D. A. and Zgrabljić Rotar, D., *Mjerodavno pravo za ugovorne odnose*, in: Josipović, T. (ed.), Privatno pravo Europske unije – Posebni dio, Narodne novine, Zagreb, 2022, pp. 217–232
3. Bjelinski Radić, I., *Kritička promišljanja o prijedlogu Direktive o poboljšanju radnih uvjeta platformskih radnika*, Zbornik Pravnog fakulteta u Zagrebu, Vol.72, No. 6, 2022, pp. 1467-1491
4. Boto, J. M. M., *Collective Bargaining and the Gig Economy: Reality and Possibilities*, in: Boto, J. M. M. and Brameshuber, E. (eds), Collective Bargaining and the Gig Economy, Hart Publishing, Oxford, 2022, pp. 3-18
5. Brown, N., Law, *Jurisdiction and the Digital Nomad: Why we need more appropriate mechanisms for determining sovereignty over disputes*, Computer Law Review International, Vol. 16, No. 2, 2015, pp. 38-43
6. Bruurs, S., *Cross-border telework in light of the Rome I-Regulation and the Posting of Workers Directive*, European Labour Law Journal, Vol. 0, No. 0, 2023, pp. 1-21
7. Campo Comba, M., *The Law Applicable to Cross-border Contracts involving Weaker Parties in EU Private International Law*, Springer, Cham, 2020
8. Cherry, M. A., *A Global System of Work, A Global System of Regulation?: Crowdwork and Conflicts of Law*, Tulane Law Review, Vol. 94, 2019, pp. 1-62
9. De Stefano, V., *Introduction: Crowdsourcing, the Gig-Economy and the Law*, Comparative Labor Law & Policy Journal, Vol. 37, No. 3, 2016, pp. 1-10
10. Gruber-Risak, M., *Classification of Platform Workers: A Scholarly Perspective*, in: Gyulavári, T. and Menegatti, E. (eds), Decent Work in the Digital Age, European and Comparative Perspectives, Hart Publishing, Oxford, 2022, pp. 85-104
11. Grušić, U., *Should the Connecting Factor of the 'Engaging Place of Business' be Abolished in European Private International Law?*, International & Comparative Law Quarterly, Vol. 62, No. 1, 2013, pp. 173-192.
12. Grušić, U., *The European Private International Law of Employment*, Cambridge University Press, Cambridge, 2015
13. Josipović, T., *Privatno pravo Europske unije – Opći dio*, Narodne novine, Zagreb, 2020
14. Kunda, I., *Međunarodnoprivatnopravni odnosi*, in: Mišćenić, E. (ed.), Europsko privatno pravo. Posebni dio., Školska knjiga, Zagreb, 2021, pp. 486–554
15. Merrett, L., *Jurisdiction over Individual Contracts of Employment*, in: Dickinson, A. and Lein, E. (eds), The Brussels I Regulation Recast, Oxford University Press, Oxford, 2015, pp. 239-253
16. Mota, C. E. and Moreno, G. P., *Article 21* in: Magnus, U. and Mankowski, P. (eds) European Commentaries on Private International Law, ECPIL, Brussels Ibis Regulation, Verlag Dr. Otto Schmidt, Köln, 2016, pp. 541-553

17. Nash, C. *et al*, *Digital Nomads Beyond the Buzzword: Defining Digital Nomadic Work and Use of Digital Technologies*, in: Chowdhury, G., *et al* (eds.), Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science, Vol. 10766, Springer, Cham, 2018, pp. 207-217
18. Naumowicz, K., *Some remarks to the legal status of platform workers in the light of the latest European jurisprudence*, Studia Z Zakresu Prawa Pracy I Polityki Społecznej, Vol. 28, No. 3, 2021, pp. 177–189
19. Pretelli, I., *A focus on platform users as weaker parties*, in: Bonomi, A. and Romano, G. P. (eds), Yearbook of Private International Law – 2020/2021, Vol. 22, Verlag Dr. Otto Schmidt, Köln, 2021, pp. 201-244
20. Ratti, L., *A Long Road Towards the Regulation of Platform Work in the EU*, in: Boto, J. M. M. and Brameshuber, E. (eds), Collective Bargaining and the Gig Economy, Hart Publishing, Oxford, 2022, pp. 39-59
21. Richter, S. and Richter, A., *Digital Nomads*, Business & Information Systems Engineering, Vol. 62, 2020, pp. 77–81
22. Rühl, G., *The Protection of Weaker Parties in the Private International Law of the European Union: A Portrait of Inconsistency and Conceptual Truancy*, Journal of Private International Law, Vol. 10, No. 3, 2014, pp. 335-358
23. Sajko, K., *Međunarodno privatno pravo*, Narodne novine, Zagreb, 2009
24. Sinander, E., *The Role of Foreseeability in Private International Employment Law*, Nordic Journal of Labour Law, Vol. 1, No. 1, 2023, p. 1-23
25. Staudinger, A., *Article 8: Individual employment contracts,* in: Ferrari, F. (ed), Rome I Regulation, Pocket Commentary, Sellier European Law Publishers, Munich, 2015, pp. 287-320
26. Tereszkiewicz, P., *Digital Platforms: Regulation and Liability in EU Law*, in: DiMatteo, L. A., Cannarsa, M., and Poncibò, C. (eds) The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge University Press, Cambridge, 2019, pp. 143–159.
27. Van Bochove, L. M., *Overriding Mandatory Rules as a Vehicle for Weaker Party Protection in European Private International Law*, Erasmus Law Review, No. 3, 2014, pp. 147-156
28. Van Calster, G., *European Private International Law*, Hart Publishing, Oxford and Oregon, 2013
29. Van Calster, G., *Of giggers and digital nomads – what role for the HCCH in developing a regulatory regime for highly mobile international employees,* in: John, T., Gulati, R., Köhler, B. (eds.), The Elgar Companion to the Hague Conference on Private International Law, Edward Elgar Publishing, Cheltenham and Northampton, 2020, pp. 464–478
30. Vukorepa, I., *Prekogranični platformski rad: zagonetke za slobodu kretanja radnika i koordinaciju sustava socijalne sigurnosti*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 70, No. 4, 2020, pp. 481-511
31. Weiss, M., *The platform economy. Tha main challenges for labour law.*, in: Mella Mendez, L. (ed.), Regulatin the Platform Economy. International Perspectives on New Forms of Work, Routledge, Oxon and New York, 2020, pp. 11-20

32. Župan, M., *Načelo najbliže veze u hrvatskom i europskom međunarodnom privatnom ugovornom pravu*, Pravni fakultet u Rijeci, Rijeka, 2006

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case 266/85 Hassan Shenavai v Klaus Kreischer [1987] ECLI:EU:C:1987:11
2. Case C-256/01 Debra Allonby v Accrington & Rossendale College [2004] ECLI:EU:C:2004:18
3. Case C-29/10 Heiko Koelzsch v État du Grand Duchy of Luxemburg [2011] ECLI:EU:C:2011:151
4. Case C-384/10 Jan Voogsgeerd v Navimer SA [2011] ECLI:EU:C:2011:842
5. Case C-64/12 Anton Schlecker v Melitta Josefa Boedeker [2013] ECLI:EU:C:2013:551
6. Case C-413/13 FNV Kunsten Informatie en Media v Staat der Nederlanden [2014] ECLI:EU:C:2014:2411
7. Case C-47/14 Holterman Ferho Exploitatie BV and Others v F.L.F. Spies von Büllesheim [2015] ECLI:EU:C:2015:574
8. Case C-603/17 Peter Bosworth and Colin Hurley v Arcadia Petroleum Limited and Others [2019] ECLI:EU:C:2019:310
9. Case C-692/19 B v Yodel Delivery Network Ltd [2020] ECLI:EU:C:2020:288
10. Joined Cases C-152/20 and C-218/20 DG and EH v SC Gruber Logistics SRL and Sindicatul Lucrătorilor din Transporturi v SC Samidani Trans SRL [2021] ECLI:EU:C:2021:600

EU LAW

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better working conditions for a stronger social Europe: harnessing the full benefits of digitalisation for the future of work COM/2021/761 final
2. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326
3. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241
4. Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work [2021] COM/2021/762 final
5. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177
6. 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) [2012] OJ L 351

LIST OF NATIONAL REGULATIONS AND ACTS

1. Crotian Immigration Act, Official Gazette No. 133/20, 114/22, 151/22
2. Spanish Law 28/2022 for the promotion of the ecosystem of emerging companies, Official Gazette No. 306

WEBSITE REFERENCES

1. Bruurs, S., *Digital Nomads and the Rome I Regulation: An Overview*, Global Workplace Law & Policy, 2022, pp. 1-7, [https://global-workplace-law-and-policy.kluwerlawonline.com/2022/12/14/digital-nomads-and-the-rome-i-regulation-an-overview/], Accessed 15 April 2023

Topic 2

Legal Education and University Management in the Digital Age

UDK 37.091.33-028.27:34
Review article

FEASIBILITY OF MOOCS FOR LEGAL EDUCATION*

Mirela Župan, PhD, Full Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
mzupan@pravos.hr

ABSTRACT

Distance learning tools are not a feature of modern times. However, COVID-19 pandemic boosted its usage and enabled its penetration into higher education. Among various e-learning features, higher education embraced model of Massive Open Online Courses (MOOCs). This paper addresses the very notion of e-learning in law. It focuses on MOOCs from the perspective of educational pedagogy, but more specifically on its usage in legal education. Pros and contras are given based on experience of MOOCs development in the framework of DIGinLaw project.

Keywords: *MOOCs, legal education, E-learning, digital literacy, digital competences*

1. INTRODUCTION

Distance learning tools are not a feature of modern times, but they evolved over the last decades. Educational sciences have intensively explored the modalities of distance learning and the use of information and communication technology (hereinafter: ICT) for teaching in higher education (hereinafter: HE). However, COVID -19 pandemic boosted its usage and enabled its penetration into HE in general. Triggered by necessity, other scientific fields have also started to explore the possibilities and challenges of using technology to teach a particular scientific field. Legal sciences are no exception to that either. All over the world during the pandemic law schools have combined high-tech and low-tech approaches to help teachers support student learning.[1] Though the delivery of lectures often did not comply with contemporary e-learning didactic and methodical approaches, the

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1 Barron, M.; Cobo, C.; Munoz-Najarinaki, A.; Ciarrusta, S., *The changing role of teachers and technologies amidst the COVID 19 pandemic: key findings from a cross-country study*, World Bank Blogs, 2021,

system worked for crisis at hand. However, the recent global study revealed that despite the e-learning movement during and after COVID-19 pandemic, most law schools returned to traditional methods of class delivery.[2] Advantages and potential challenges of distance learning in the field of law should be explored, to enable full benefits of technology for law students and legal profession in general.

Distance learning tools are not creation of modern times. The concept of e-learning has been developing systematically for several decades. The development dates back to the 1980s when computers were gradually introduced into the education system. Introduction of the Internet in the 1990s strengthened the e-learning architecture. Further momentum in development continued in the 2000s with the emergence of social networks, Google Scholar and cloud computing around 2010[3] and open Educational resources around 2020s. Among various e-learning features, contemporary high education embraced the model of Massive Open Online Courses (MOOCs). This paper addresses the very notion of MOOCs from perspective of educational pedagogy. More specifically, it focuses on the methodology of MOOCs creation and its performance in area of legal education. Pros and contras are given based on experience of MOOCs development in the framework of *Time to Become Digital in Law* project (DIGinLaw).[4]

Time to Become Digital in Law project (2020-1-HR01-KA226-HE-094693) is funded by the EU through *Erasmus+ KA226 - Partnerships for Digital Education Readiness 2020 programme.* DIGinLaw is a collaborative project run by a consortium of four European universities: Josip Juraj Strossmayer University of Osijek (Croatia) (coordinator), University of Milano (Italy), University Court of the University of Aberdeen (United Kingdom) and Computing Centre of University of Zagreb (Croatia) as partners. DIGinLaw raises awareness of digital demands in HE in law and fosters the creation of digital literacy and digital competence that is needed in the law labour market. Project is thereby creating an open and inclusive society of legal knowledge to scientific area dealing with the effects of digitalization on law and legal education.

[https://blogs.worldbank.org/education/changing-role-teachers-and-technologies-amidst-covid-19-pandemic-key-findings-cross], Accessed 25 August 2023.

2 Nottage, L.; Ibusuki, M., *Comparing Online Legal Education World-Wide: An Overview Before and after the Pandemic*, in: Nottage, L.; Ibusuki, M. (eds.), Comparing Online Legal Education, Intersentia, Cambridge, 2023.

3 Cope, B.; Kalantzis, M., *Pedagogies for Digital Learning: From Transpositional Grammar to the Literacies of Education*, in: Sindoni, M. G.; Moschini, I. (eds.), Multimodal Literacies Across Digital Learning Contexts*,* Routledge, New York, 2021, pp. 34-53.

4 Time to Become Digital in Law, *MOOCs,* [https://www.pravos.unios.hr/diginlaw/modules/], Accessed 27 August 2023.

2. IMPACT OF DIGITAL TRANSFORMATION ON LEGAL PROFESSION

Digital education synonyms for e-learning and learning based on the application of ICT in the teaching and learning process. Since it is a model of education based on the application of digital technologies, performance is possible entirely in the form of online learning or through other forms of mixed teaching which include a combination of classical teaching and the application of ICT. E-learning availability is boosted by the deployment of a wide range of digital technologies such as apps, platforms, software and others. Digital transformation as a change related to the application of digital technology in all aspects of human life, has undeniable potential in legal education.[5] Moreover, it's a demand posted by the legal profession which is getting digitalized.

The legal profession is already in the third stage of the digital transformation. The first stage began in the late 1970s with electronic data processing and computing, primarily using computer solutions for the creation and processing of text and data storage media.[6] This was followed by a second stage characterised by the use of large data (big data) and modern telecommunications. Within this stage, the technology-enabled lawyers and other legal professionals to accumulate and process an increasing amount of legal material through the storage and decentralisation of data in the "cloud". In addition, at this stage, some outdated information and communication solutions have been abandoned. Practitioners have increasingly focused on the use of e-mail, as well as video conferencing systems that enable more direct virtual communication in real time.[7] Finally, the legal profession is currently in the third stage of its digital transformation, characterised by the use of artificial intelligence, algorithms and automated decision-making systems. Although there is global disparity in the level of development of the third stage of digital transformation of the legal profession, automated court systems already perform full judicial functions in some countries.[8] The rise of modern technology has changed the concept of technological literacy. Therefore, online legal educational patterns should exceed low-level assessment, as future lawyers must learn to deal with artificial inteligence,[9] digital assets, blochain and many other.[10]

---

5 Janssen A.; Vennmanns, T.; *The Effects of Technology on Legal Practice: From Punch Card to Artificial Intelligence*?, in Dimatteo, L.A. et al (eds.), The Cambridge Handbook of Lawyering in the Digital Age, Cambridge University Press, Cambridge – New York, 2021, p. 59.

6 *Ibid.,* pp. 46-47.

7 *Ibid.,* pp. 48-49.

8 *Ibid.,* p. 49.

9 McGinnis J. O.; Pearce, R. G.; *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, Fordham Law Review, Vol. 82, No. 6., 2014, pp. 3041-3042.

10 Fenwick, M.; Wulf A. Kaal & Erik P. M. Vermeulen, *Legal Education in a Digital Age*, in: Compagnucci, C.M.; Forgó, N.; Kono, T.; Teramoto, S.; Vermeulen, E.P.M. (eds.), Legal Tech and the New Shar-

In view of the above, the need for the digital transformation of HE in the field of law is also necessary for HE institutions to fulfil their social function and to educate competing and digitally competent lawyers for the labour market. All the more so, according to the given normative framework, the qualifications obtained by completing university studies should, *inter alia*, confirm the competence to live and work in a changing social context in accordance with the requirements of modern information and communication technologies. Digitalization becomes vital for providing lifelong-learning in law as well. [11]

3. EUROPEAN STRATEGICAL INCENTIVE TO BOOST E-LEARNING IN LAW

The most prominent form of online education is the creation of MOOCs. However, leading MOOC platforms are outside the European Union (hereinafter: EU). In Europe, there is a diverse range of online courses offered, but very few MOOCs. Given the good Internet coverage and high GDP of EU Member States, but also a number of strategic goals set by the EU, the digitalization of HE should be implemented systematically. Many strategic goals speak for legal education delivered by MOOCs.

The European Digital Strategy[12] is promoted through the programmes A Europe fit for the digital age, Empowering people with a new generation of technologies,[13] 2030 Digital Compass: the European way for the Digital Decade,[14] and financially supported by the Next Generation EU.[15] E-learning in HEshould meet the desired future investment in digital skills for all Europeans and directly contribute to achieving an open, democratic and sustainable society that harnesses technology in order to reach the milestone of Europe to become climate-neutral by 2050.

---

ing Economy, Springer Nature, 2023, pp. 135–154.

11 Župan, M.; Kunda, I.; Poretti, P.; *Judicial Training in European Private International Law in Family and Succession Matters*, in: Pfeiffer, T.; Lobach, Q. C.;Rapp, T. (eds.), Facilitating Cross-Border Family Life – Towards a Common European Understanding: EUFams II and Beyond, Heidelberg University Publishing, Heidelberg, 2021, pp. 122-124.

12 European Commission, *European Digital Strategy*, 2020, [https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy], Accessed 27 August 2023.

13 European Commission, *A Europe fit for the digital age, Empowering people with a new generation of technologies*, 2020, [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en], Accessed 27 August 2023.

14 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2021) 118 final.

15 European Union, *Next Generation EU*, [https://europa.eu/next-generation-eu/index_en], Accessed 27 August 2023.

MOOCs usage in HE is in line with European Digital Education Action Plan 2021-2027[16] priorities on fostering high performing digital education ecosystem and enhancing digital skills and competences for the digital transformation. With its priority two, the Digital Education Action Plan 2021-2027 redefines education and training for the digital age and goes in line with a European Skills Agenda.[17] Using MOOCs for education meets European Declaration on Digital Rights and Principles for the Digital Decade and Digital Decade Policy Programme 2030.[18]

European Strategy for Universities[19] gives universities a fundamental role in digital transformation. MOOCs thus go hand in hand with the European Commission's science and knowledge service advocacy for Open Educational Resources (hereinafter: OER). OER are […] learning, teaching, and research materials in any format and medium that reside in the public domain or are under copyright that have been released under an open license, permitting no-cost access, re-use, repurposing, adaptation, and redistribution by others.[20] Delivery of MOOC's also contributes to achieving a micro-qualifications advocated by the EU.[21]

The use of digital tools meets the Council's Recommendation of 16 June 2022 on learning for green transition and sustainable development.[22] EU goals are to achieve an open, democratic and sustainable society that takes advantage of technology to reach the milestone of Europe becoming climate-neutral by 2050. MOOCs contribute to realization of Green Deal objectives by learning in virtual environment and reducing travel and use of consumables.

---

16 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digital Education Action Plan 2021-2027 Resetting education and training for the digital age COM/2020/624 final.

17 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience COM/2020/274 final.

18 European Union, *Declaration on European Digital Rights and Principles*, 2022, [https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration], Accessed 28 August 2023.

19 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European strategy for universities COM(2022) 16 final.

20 Cronin, C.; *Openness and Praxis: Exploring the Use of Open Educational Practices in Higher Education*, Int. Rev. Res. Open Distrib. Learn. Vol. 18, No. 5, 2017, pp. 1–21.

21 Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02 ST/9790/2022/INIT [2022] *OJ C 243, pp. 10–25.*

22 Council Recommendation of 16 June 2022 on learning for the green transition and sustainable development 2022/C 243/01 (Text with EEA relevance) ST/9795/2022/INIT [2022] *OJ C 243, pp. 1–9.*

MOOCs in open access further contribute to knowledge even more accessible and education more inclusive. MOOCs reduce geographic and economic barriers with education accessible to all. MOOCs in particular contributes to the achievement of the EU disability policy by providing the inclusive learning.[23] Approximately more than 87 million people in the EU have some kind of disability, which to a certain extent limits their participation in social and economic life.

In terms of lifelong learning in the field of legal education, the goals of EU justice policy touch on digitalisation. The European Commission's Communication of 27 May 2020 entitled "Europe's Moment: Repair and Prepare for the Next Generation" affirms that digitalisation of justice systems can improve access to justice and the operation of the business environment. The aim of the Strategy on e-Justice 2019-2023 is to improve and simplify access to information in the field of justice, support the digitalisation of cross-border judicial and extrajudicial procedures in all areas of law.[24]

Law students with developed digital competences are an invaluable asset for the labour market. Quality future lawyers holding competitive digital competences and skills are able to respond to the needs of clients, law firms and the court system. Transferable digital competences and skills acknowledged by the European Qualification Framework (EQF) foster free circulation of highly educated labour market.[25] The need for new digital skills in law labour market stands out of the New Strategy on European Judicial Training for 2021-2024 as well.[26] It asks for development of tailored e-learning addressing the needs of EU judicial space: interactive, practical and accessible to all learners.

"Digital sources of knowledge are becoming increasingly accessible to students and adults. Teachers, counsellors, mentors and trainers therefore need to develop the ability to introduce new approaches through information and communication technologies (and related tools) and create new digital educational content. For this reason, continuing professional development will be vital for all teachers and

---

23 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Union of Equality: Strategy for the Rights of Persons with Disabilities 2021-2030 COM/2021/101 final.

24 [2019] OJ C 96/3.

25 The European Qualifications Framework: supporting learning, work and cross-border mobility, Publications Office of the European Union, Luxembourg, 2018.

26 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Ensuring justice in the EU — a European judicial training strategy for 2021-2024 COM/2020/713 final.

educational staff in the process of identifying, developing and guiding the knowledge, skills and abilities of individuals."[27]

A European framework for digital educational content[28] seeks to establish main principles for certain education sectors and their needs. It takes into account the high-quality teaching, planning, accessibility, recognition and multilingualism. Systematic development of digital education is complemented by an idea of setting up a European platform for the exchange of certified online resources.[29] It reflects the need for interoperability, certification, verification and portability of content by establishing mass open online courses and linking existing educational platforms.

The introduction of innovative digital HE models is advocated also by European Universities Initiative,[30] where EU inter-university campuses will function virtually and in a physical environment.[31] Another contribution to facilitating secure electronic exchange and verification of student data and ratings and facilitating student mobility management comes with the European student card Initiative.[32] Identification and authentication for online learning activities in a host institution in another Member State is based on EU electronic identification rules.[33]

4. MOOC'S AS A FEATURE OF E-LEARNING IN LAW

Educational sciences have been deeply engaged with the phenomena of online and distance learning. However, the penetration of online education into other HE areas requires scientist and teachers of certain fields of science to reconsider and redefine the way they transpose knowledge in a virtual environment. Legal educa-

---

27 *Ibid.,* p. 35.

28 European Commission, *European Framework for Digitally Competent Educational Organisations – DigCompOrg*, [https://joint-research-centre.ec.europa.eu/european-framework-digitally-competent-educational-organisations-digcomporg_en], Accessed 28 August 2023.

29 European Commission, *European Education Area, Quality education and training for all*, [https://education.ec.europa.eu/resources-and-tools/online-learning-resources/online-platforms], Accessed 28 August 2023.

30 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European strategy for universities Strasbourg, COM(2022) 16 final.

31 CIVIS, *European University Initiative: transforming higher education in Europe*, [https://civis.eu/en/about-civis/european-university-initiative], Accessed 28 August 2023.

32 European Commission, *European Student Card Initiative*, [https://education.ec.europa.eu/education-levels/higher-education/european-student-card-initiative], Accessed 28 August 2023.

33 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257, pp. 73–114.

tion theory has to critically address basic underlying features of online education, referred to as phenomena of e-learning ecologies.[34] A number of new educational technologies are emerging in both traditional and modern learning venues. The concept, cost and benefits of online HE have occupied academia during the last decade, with recent academic assessment dealing with online HE in general[35] and in law.[36] Recently the methodology of e-lerning in law gets more elaborated.[37] In order to facilitate the digital transformation of HE, varied tools and guides are developed.[38] Despite of it, representation of MOOCs in curricula (regular or optional) of European law schools is scarce.

4.1. DIGinLaw project – pilot MOOCs in law

The *Time to become digital in law* – DIGinLaw project is the most prominent example of a progressive, thorough and well-established approach to online legal education.[39] The project aims to address aspects of digitalisation in legal education and law. It addresses the development of digital competencies of HE teachers for innovative teaching practices, which are the backbone of the module on knowledge, skills and competencies for T-shaped lawyers. As a result, 12 MOOCs have been developed in collaboration with four participating universities. Digital competencies for lifelong learning for law students are also being developed. In addition to digital skills, the promotion of research and publication on the topic "Digitalisation in legal education and law" lies on the open science foundation.

Project partners developed 11 MOOCs corresponding to EQF level 7 and 1 joint MOOC for PhD level 8. MOOCs for level 7 touch upon content which is mainly still not part of regular curricula. Topics covered are: Cross-border Dispute Reso-

---

[34] Cope, B.; Kalantzis, M., (eds.), *E-Learning Ecologies, Principles for New Learning and Assessment,* Routledge, Oxon – New York, 2017.

[35] Fandl, K. J.; Smith, J. D., *Success as an Online Student: Strategies for Effective Learning*, Routledge, Oxon – New York, 2013.; Isaias, P.; Sampson, D. G.; Ifenthaler, D. (eds.), *Online Teaching and Learning in Higher Education*, Springer, Cham, 2020; McKenzie, S.; Garivaldis, F.; Dyer, K. R., *Tertiary Online Teaching and Learning: TOTAL Perspectives and Resources for Digital Education*, Springer, Cham, 2020; McDougall, J., *Critical Approaches to Online Learning*, Critical Publishing, 2021; Kučina Softić, S.; Odak, M.; Lasić Lazić, J.; *Digitalna transformacija - nove prilike i izazovi u obrazovanju,* Sveučilište Sjever, Koprivnica, 2021, p. 207.

[36] Jones, E.; Cownie, F.; *Key Directions in Legal Education: National and International Perspectives*, Routledge, Oxon – New York, 2020.

[37] Thanaraj, A.; Gledhill, K., (eds.), *Teaching Legal Education in the Digital Age. Pedagogical Practices to Digitally Empower Law Graduates*, Routledge, Oxon – New York, 2023.

[38] Inamorato Dos Santos, A.; Punie, Y.; Castaño Muñoz, J., *Opening Up Education: A Support Framework for Higher Education Institutions*, Publications Office of the European Union, Luxembourg, 2016.

[39] Time to Become Digital in Law, [https://www.pravos.unios.hr/diginlaw], Accessed 28 August 2023.

lution in a Digital World; Data protection and cybersecurity in the EU; Consumer Protection in a Digital Age; Artificial Intelligence and Criminal Justice; International Family Law in the Age of Modern Technologies, Algorithmic discrimination: a blueprint for a legal analysis; Cryptocurrencies and Conflict of Laws; Managing Economic Aspects of Cross-Border Families in the Digital Era; Distributed Ledger Technologies and EU Private International Law; Free Movement of Persons in a Digital World; Human Rights Challenges in the Digital Era.[40] In additions, project has resulted with two MOOCs targeting digital competences of law students and law professors.

4.2. MOOC's revealed – call for a new pedagogical approach

Online education requires a change in pedagogical approaches that accompany e-learning and use of computers. There is a high risk of delivering online classes without appropriate methodology.[41] Rate of satisfaction with online classes reflects the attitudes of students towards online teaching in HE. Thus lack of appropriate methodology can lead to reservations or barriers and result in insufficient usage.[42]

The implementation of e-learning in the educational process enables a paradigm shift from the teacher being at the centre of the educational process to the student being the centre of the educational process. The teacher is thus afforded a new role of mentor and coordinator in the educational process, with students becoming active participants and taking responsibility for their results in the educational process, in both the transfer and creation of knowledge and research. Reversal of the traditional teacher–learner role calls for a new approach. Technology interventions have improved teacher engagement with students. Effective teachers rely on improved access to content, data and networks to better support student learning. Integrating e-learning into the regular education system is preconditioned by teachers developing digital competencies. This requires investment in the development of didactic-methodological resources and capacities to exploit the full potential of remote and blended learning.[43]

---

40 Time to Become Digital in Law, *MOOCs*, [https://www.pravos.unios.hr/diginlaw/modules/], Accessed 30 August 2023.

41 Bennett, R.; Kent, M., (eds.), *Massive Open Online Courses and Higher Education: What Went Right, What Went Wrong and Where to Next?,* Routledge*, Oxon – New York*, 2017.

42 Constantino, G.D.; Raffagheli, J.E., *Online teaching and learning, going beyond the information given*, in: Di Gesú, M. G.; González M.F. (eds), Cultural Views on Online Learning in Higher Education: A Seemingly Borderless Class, Springer Nature, Cham, 2021, p. 4.

43 Kučina Softić, S., *Teachers' digital competencies for E-learning application in higher education*, in: Towards Personalized Guidance and Support for Learning, Proceedings of the 10thEuropean Distance and E-Learning Network Research Workshop, Barcelona, 24-26 October 2018, 2018, p. 206.

There is a growing focus on learning processes, with students becoming active participants responsible for their learning achievements, and teachers using innovative teaching methods, encouraging students and motivating them to get involved, explore, reflect, build new knowledge and acquire new skills. Traditional teaching methods, primarily with the teacher at the centre of the educational process are insufficient for today's students. It does not meet their needs as students to learn individually. Technology enables and encourages a paradigm shift in focus from teaching to learning, and provides a model for student placement at the centre of the educational process. Digital technologies in teaching and learning are changing the skills teachers must have and shifting the focus from teaching design to learning design, changing the teacher's perspective from a sage on the stage to a guide and tutor.[44] The role of the teacher changes from a synthesiser of disciplinary content to a digital content curator who designs learning activities.[45]

5. METHODOLOGICAL CHALLENGES TO MOOCS IN LAW

MOOCs can be self-paced, fully online, or guided.[46] The digital environment calls for a new approach to defining student activities and achieving desired learning outcomes.[47] Students must be provided with adequate learning materials. Adequacy is measured by several criteria. In terms of availability, it is necessary to create digital materials[48] or use open access materials.[49] Though OER are much prompted by the EU,[50] experience of DIGinlaw project proved that very accurate legal content reading materials are mainly not available in open access. Even if available, scientific papers are mainly not appropriate for MOOCs reading materials. Namely, the complexity and quantity of learning materials depends on the education level. In line with the EQF guidelines, the number of pages in a given

---

44 Dysart T.L.; Norton, T.; *Law Teaching Strategies for a New Era: Beyond the Physical Classroom*, Carolina Academic Press, LLC, 2021.

45 Sindoni, M. G.; Moschini, I.; (eds.), *Multimodal Literacies Across Digital Learning Contexts*, Routledge, Oxon – New York, 2021; Cope; Kalantzis, *op. cit.*, note 3, p. 7.

46 Armellini, A.; Padilla Rodriguez, B.C., *Active Blended Learning: Definition, Literature Review, and a Framework for Implementation*, in: Padilla Rodriguez, B.C.; Armellini, A. (eds.), Cases on Active Blended Learning in Higher Education, IGI Global, 2021.

47 Gil-Jaurena, I.; Kučina Softić, S., *Aligning learning outcomes and assessment methods: a web tool for e-learning courses*, International Journal of Educational Technology in Higher Education, Vol. 13, 17, 2016.

48 Rubin, E., *Legal Education in the Digital Age*, Cambridge University Press, Cambridge, 2012.

49 Kučina Softić, S.; Rako, S.; *Otvoreno obrazovanje i otvoreni obrazovni sadržaji*, in: Hebrang Grgić, I., (ed.), *Otvorenost u znanosti i visokom obrazovanju*, Školska knjiga, Zagreb 2018.

50 Mićunović, M.; Rako, S.; Feldvari, K., *Open Educational Resources (OERs) at European Higher Education Institutions in the Field of Library and Information Science during COVID-19 Pandemic*, Publications 2023, Vol. 11, No. 3, 38, 2023.

reading material should be calculated through the time a student is expected to spend reading and learning. HE teachers should develop digital competencies. The know-how is available with an open access MOOC on digital competence for law teachers.[51]

MOOCs are divided into sections (weeks of performance) that have a similar/equal workload. The sections usually consist of a video, interactive material, PPT or some other digital tool, student assignments, reading materials and assessment. The teacher must specify the time required for accomplishing each section or each task within a section. MOOCs can be self-paced, fully online, or guided.[52] The latter is advocated by active blended learning, where the course includes static materials for reading and self-paced forms of e-learning, where students can watch or otherwise participate, and parts that are directly instructed by the teacher – guided.[53]

The new environment calls for a new approach to defining student activities and achieving the desired learning outcomes.[54] However, as MOOCs can be self-paced or guided, the choice of model would largely determine student activities as well as the assessment strategy. From a legal perspective, the usual distance platform tools for knowledge assessment, multiple choice questions, blank questions, quizzes, crossword puzzles, etc., should be appropriate for student self-assessment. However, students should be encouraged to solve tasks in interactive ICT programmes licenced for education, such as those whose goal is to create a mental map. Solving a hypothetical case can be a very promising student activity, although it would be advisable to give students hints and problem questions, or even provide them with a teacher essay in a step-by-step build-up of case complexity. The teacher may come up with even more complex team collaboration tools, or at least set up a forum so that students who sign up for the course can interact. Sometimes problem issues/hypothetical cases are given as assignments that require a student to write a response (approximately 200 words) and upload it to the forum for others to read and discuss. If this option is used, a time frame must be specified. Such assignment is preferable in guided courses. In a guided course, it is preferable to activate students to collaborate, use interactive tools for that purpose, schedule a debate, and assign them an essay on a topic or an elaboration of case law.

---

51 MoD, [mod.srce.hr], Accessed 30 August 2023.

52 Armellini; Padilla Rodriguez, *op. cit.*, note 46.

53 Carl, M.; Worsfold, L., *The implementation and embedding of digital skills and digital literacy into the curriculum considering the Covid-19 pandemic and the new SQE: A case study from inception to implementation and continual development of the Digital Academy*, Journal of Information Literacy, Vol. 15, No. 3, 2021, pp. 119-133 and pp. 121-122.

54 Gil-Jaurena; Kučina Softić, *op. cit.,* note 47.

Students must be provided with adequate learning materials. Adequacy is measured by several criteria. In terms of availability, it is necessary to create digital materials[55] or use open access.[56] Complexity and quantity of learning materials depend on the level of education. In line with the EQF guidelines, the number of pages in a given reading material should be calculated through the time a student is expected to spend reading and learning. An average student can read 10 pages and study 6.25 pages of difficult professional text, or read 15 pages and study 7-8 pages of simpler professional text as individual tasks/team work in one work hour.

As a reward for participating in a MOOC, a student can receive a digital badge or ECTS credits. If ECTS credits are formally awarded for the course, the hours of work per 1 ECTS are calculated according to the national scale, which is in principle 25-30 student work hours for 1 ECTS.

6. CONCLUSION

Digitalization strongly affects all segments of society including science and the transfer of knowledge. Digital technology may provide high-quality and inclusive education and training. Such technology may support the teaching and learning process either as fully online, distance or blended learning. It boosts more personalised and flexible learners-centred learning. E-learning enables acquiring digital competences (knowledge, skills and attitudes) for life, work, learning and advancement in an increasingly digital-dependent world. The need to set up new teaching and learning facilities in legal education can be extracted from European strategic documents on digitalisation, high education, green deal, disability, sills and competences and judicial training as well.

Focusing more specifically on the legal profession and HE in law, developing high level MOOCs in law is necessary and beneficial for many reasons. Increased digitalization has changed the way legal services are conducted. Future lawyers ought to be competent and skilled to meet the needs of their clients, law firms and the court system. Knowledge delivery by MOOCs contributes to digitalized legal education with transferable digital competences and skills recognized by EQF. However, the lack of specific methodology in an e-course creation and performance caused by insufficient digital competences of the HE lecturers may impede the full capacity of legal knowledge transfer in a virtual environment. Implementing e-learning in legal education requires the systematic approach. It asks for the reassessment of the need for innovation in law learning methodology, need to departure towards open

[55] Rubin, *op. cit.*, note 48.

[56] Kučina Softić; Rako, *op. cit.,* note 49.

and inclusive education grounded on e-learning, need to involve modern technology to HE process, need to advance digital skills of law teachers and law students, the need to deliver T(echnology)-shaped lawyers to the labour market. In terms of curricula, it asks for an in-depth assessment while technology does not affect all aspects of law and legal branches equally, but is innate to some.

REFERENCES

BOOKS AND ARTICLES

1. Armellini, A.; Padilla Rodriguez, B.C., *Active Blended Learning: Definition, Literature Review, and a Framework for Implementation*, in: Padilla Rodriguez, B.C.; Armellini, A. (eds.), Cases on Active Blended Learning in Higher Education, IGI Global, 2021, pp. 1-22
2. Bennett, R.; Kent, M., (eds.), *Massive Open Online Courses and Higher Education: What Went Right, What Went Wrong and Where to Next?,* Routledge*, Oxon – New York*, 2017
3. Carl, M.; Worsfold, L., *The implementation and embedding of digital skills and digital literacy into the curriculum considering the Covid-19 pandemic and the new SQE: A case study from inception to implementation and continual development of the Digital Academy*, Journal of Information Literacy, Vol. 15, No. 3, 2021, pp. 119-133
4. Cope, B.; Kalantzis, M., (eds.), *E-Learning Ecologies, Principles for New Learning and Assessment,* Routledge, Oxon – New York, 2017
5. Cope B.; Kalantzis, M., *Pedagogies for Digital Learning: From Transpositional Grammar to the Literacies of Education*, in: Sindoni, M. G.; Moschini, I. (eds.), Multimodal Literacies Across Digital Learning Contexts*,* Routledge, New York, 2021, pp. 34-53
6. Constantino, G.D.; Raffagheli, J.E., *Online teaching and learning, going beyond the information given*, in: Di Gesú, M. G.; González, M.F. (eds.), Cultural Views on Online Learning in Higher Education: A Seemingly Borderless Class, Springer Nature, Cham, 2021, pp. 3-28
7. Cronin, C.; *Openness and Praxis: Exploring the Use of Open Educational Practices in Higher Education*, Int. Rev. Res. Open Distrib. Learn. Vol. 18, No. 5, 2017, pp. 1–21
8. Dysart T.L.; Norton, T.; *Law Teaching Strategies for a New Era: Beyond the Physical Classroom*, Carolina Academic Press, LLC, 2021
9. Fandl, K. J.; Smith, J. D., *Success as an Online Student: Strategies for Effective Learning*, Routledge, Oxon – New York, 2013
10. Fenwick, M.; Wulf A. Kaal & Erik P. M. Vermeulen, *Legal Education in a Digital Age*, in: Compagnucci, C.M.; Forgó, N.; Kono, T.; Teramoto, S.; Vermeulen, E.P.M. (eds.), Legal Tech and the New Sharing Economy, Springer Nature, 2023, pp. 135–154
11. Gil-Jaurena, I.; Kučina Softić, S., *Aligning learning outcomes and assessment methods: a web tool for e-learning courses*, International Journal of Educational Technology in Higher Education, Vol. 13, 17, 2016, pp. 1-16
12. Isaias, P.; Sampson, D. G.; Ifenthaler, D. (eds.), *Online Teaching and Learning in Higher Education*, Springer, Cham, 2020
13. Janssen A.; Vennmanns, T.; *The Effects of Technology on Legal Practice: From Punch Card to Artificial Intelligence*?, in Dimatteo, L.A. et al (eds.), The Cambridge Handbook of Lawyer-

ing in the Digital Age, Cambridge University Press, Cambridge – New York, 2021, pp. 38-56

14. Jones, E.; Cownie, F.; *Key Directions in Legal Education: National and International Perspectives*, Routledge, Oxon – New York, 2020
15. Kučina Softić, S., *Teachers' digital competencies for E-learning application in higher education*, in: Towards Personalized Guidance and Support for Learning, Proceedings of the 10thEuropean Distance and E-Learning Network Research Workshop, Barcelona, 24-26 October 2018, 2018, pp. 203-212
16. Kučina Softić, S.; Odak, M.; Lasić Lazić, J.; *Digitalna transformacija - nove prilike i izazovi u obrazovanju,* Sveučilište Sjever, Koprivnica, 2021
17. Kučina Softić, S.; Rako, S., *Otvoreno obrazovanje i otvoreni obrazovni sadržaji*, in: Hebrang Grgić, I. (ed.), *Otvorenost u znanosti i visokom obrazovanju*, Školska knjiga, Zagreb, 2018, pp. 131-143
18. McDougall, J., *Critical Approaches to Online Learning*, Critical Publishing, 2021
19. McGinnis J. O.; Pearce, R. G.; *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, Fordham Law Review, Vol. 82, No. 6., 2014, pp. 3041-3066
20. McKenzie, S.; Garivaldis, F.; Dyer, K. R., *Tertiary Online Teaching and Learning: TOTAL Perspectives and Resources for Digital Education*, Springer, Cham, 2020
21. Mićunović, M.; Rako, S.; Feldvari, K., *Open Educational Resources (OERs) at European Higher Education Institutions in the Field of Library and Information Science during COVID-19 Pandemic*, Publications 2023, Vol. 11, No. 3, 38, 2023, pp. 1-26
22. Nottage, L.; Ibusuki, M., *Comparing Online Legal Education World-Wide: An Overview Before and after the Pandemic*, in: Nottage, L.; Ibusuki, M. (eds.), Comparing Online Legal Education, Intersentia, Cambridge, 2023
23. Rubin, E., , *Legal Education in the Digital Age*, Cambridge University Press, Cambridge, 2012
24. Sindoni, M. G.; Moschini, I.; (eds.), *Multimodal Literacies Across Digital Learning Contexts*, Routledge, Oxon – New York, 2021
25. Thanaraj, A.; Gledhill, K., (eds.), *Teaching Legal Education in the Digital Age. Pedagogical Practices to Digitally Empower Law Graduates*, Routledge, Oxon – New York, 2023
26. Župan, M.; Kunda, I.; Poretti, P., *Judicial Training in European Private International Law in Family and Succession Matters*, in: Pfeiffer, T.; Lobach, Q. C.;Rapp, T. (eds.), Facilitating Cross-Border Family Life – Towards a Common European Understanding: EUFams II and Beyond, Heidelberg University Publishing, Heidelberg, 2021, pp. 91-149

EU LAW

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2021) 118 final
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digital

Education Action Plan 2021-2027 Resetting education and training for the digital age, COM/2020/624 final

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience, COM/2020/274 final
4. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European strategy for universities COM(2022) 16 final
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Ensuring justice in the EU — a European judicial training strategy for 2021-2024 COM/2020/713 final
6. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Union of Equality: Strategy for the Rights of Persons with Disabilities 2021-2030 COM/2021/101 final
7. Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02 ST/9790/2022/INIT [2022] OJ C 243
8. Council Recommendation of 16 June 2022 on learning for the green transition and sustainable development 2022/C 243/01 (Text with EEA relevance) ST/9795/2022/INIT [2022] OJ C 243
9. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257
10. The European Qualifications Framework: supporting learning, work and cross-border mobility, Publications Office of the European Union, Luxembourg, 2018

REPORTS

1. Inamorato Dos Santos, A.; Punie, Y.; Castaño Muñoz, J., *Opening Up Education: A Support Framework for Higher Education Institutions*, Publications Office of the European Union, Luxembourg, 2016

WEBSITE REFERENCES

1. Barron, M.; Cobo, C.; Munoz-Najarinaki, A.; Ciarrusta, S., *The changing role of teachers and technologies amidst the COVID 19 pandemic: key findings from a cross-country study*, World Bank Blogs, 2021, [https://blogs.worldbank.org/education/changing-role-teachers-and-technologies-amidst-covid-19-pandemic-key-findings-cross], Accessed 25 August 2023
2. CIVIS, *European University Initiative: transforming higher education in Europe*, [https://civis.eu/en/about-civis/european-university-initiative], Accessed 28 August 2023
3. European Commission, *A Europe fit for the digital age, Empowering people with a new generation of technologies*, 2020, [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en], Accessed 27 August 2023

4. European Commission, *European Digital Strategy*, 2020, [https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy], Accessed 27 August 2023
5. European Commission, *European Education Area, Quality education and training for all*, [https://education.ec.europa.eu/resources-and-tools/online-learning-resources/online-platforms], Accessed 28 August 2023
6. European Commission, *European Framework for Digitally Competent Educational Organisations – DigCompOrg*, [https://joint-research-centre.ec.europa.eu/european-framework-digitally-competent-educational-organisations-digcomporg_en], Accessed 28 August 2023
7. European Commission, *European Student Card Initiative*, [https://education.ec.europa.eu/education-levels/higher-education/european-student-card-initiative], Accessed 28 August 2023
8. European Union, *Declaration on European Digital Rights and Principles*, 2022, [https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration], Accessed 28 August 2023
9. European Union, *Next Generation EU*, [https://europa.eu/next-generation-eu/index_en], Accessed 27 August 2023
10. MoD, [mod.srce.hr], Accessed 30 August 2023
11. Time to Become Digital in Law, [https://www.pravos.unios.hr/diginlaw], Accessed 28 August 2023
12. Time to Become Digital in Law, *MOOCs*, [https://www.pravos.unios.hr/diginlaw/modules/], Accessed 30 August 2023

UDK 316.774:37.03
Review article

DEEP DIVE INTO THE MEDIA WORLD OF YOUTH*

Martina Mikrut Nađsombat, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
mmikrut@pravos.hr

Ivna Tomičić, Master of Economics
Smart Counselling Marketing Agency
Gundulićeva 5, 31 000 Osijek, Croatia
ivna.tomicic@smartcon.hr

ABSTRACT

The emergence of internet technologies and social media platforms has affected all aspects of life, especially among younger generations. In this new media world of social media, for stakeholders dealing with the 15–24-year-old population it is important to understand how to communicate and engage with them. Using a combination of qualitative/quantitative research methodology, this paper aims to provide a comprehensive, descriptive view of the values, perception, and behaviour of youth (15–24) in Croatia when it comes to digital media channels and especially social media. Research results confirmed that social networks, messaging services and browsing internet are the dominant activities of young generation. YouTube, Instagram, and Facebook are the most popular social network, and principals in content creation are authenticity, customization, and interactivity. These results should serve as a basis for communication strategies within this target audience. And since the way young use social networks and create/consume content changes daily, legal framework should follow.

Keywords*: Youth 15-24, qualitative/quantitative research, descriptive analysis, social media usage*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

Change in the media landscape is constant, but we are witnessing the greatest changes in media history, especially among the young population. Young people are growing up in a completely new digital environment. Whole new world of social media evolved. It is getting more and more complex for businesses and marketing industry to make communication strategies and media channels optimization when communicating with young people. The speed of change in technology, communication channels, ways of creating and consuming content, making decisions, new business models of the social network industry... requires up-to-date reactions in creating relevant legal frameworks. Therefore, for the legal profession to respond to the challenges of emerging issues related to the development of the use of social networks, it is important to understand how and why young people, as a population that is the bearer of change, use them. Platforms and applications that are used "for free" in the social network industry are of foreign origin, and there are no borders in social network communication, so legal issues are wider than Croatian borders as well.

2. THEORETICAL BACKGROUND

The rise of social media is an extraordinary example of how quickly and drastically social behaviours can change: Something that is today part of the everyday life of one-third of the world population was unthinkable less than a generation ago.[1] The term "social media" (SM) was first used in 1994 on a Tokyo online media environment, called Matisse. It was in these early days of the commercial Internet that the first SM platforms were developed and launched. Over time, both the number of SM platforms and the number of active SM users have increased significantly, making it one of the most important applications of the Internet. Furthermore, there are big differences in social media usage over time: before 2010, SM was commonly approached as a tool of connectivity for people with common interests. After 2010, the focus changed to creating and sharing user-generated content.[2] Some studies from 2010 already pointed out the importance of considering platform and access mechanism when researching online social networks and that even the difference in level of access means that the experiences are quite distinct; the type of access transforms a longer-lasting, thorough experience, exploring pictures and other people's details, to a lightweight experience, a simple

---

1 Ortiz-Ospina, E., *The rise of social media, Our World in Data*, 2019, [https://ourworldindata.org/rise-of-social-media], Accessed 10 June 2023.

2 Aichner, T.; Grünfelder, M.; Oswin Maurer, O.; Jegeni, D., *Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019*, Cyberpsychology, Behavior, and Social Networking, Vol. 24, No. 4., 2021, pp. 215-222.

checking of status and personal messages. It is therefore essential to examine online social network use in relation to these new technologies and from a more holistic viewpoint.[3] In reviewing the social media ecosystem and considering where it is heading in the context of consumers and marketing practice, it is concluded that this is an area that is very much still in a state of flux. The future of social media in marketing is exciting, but also uncertain. If nothing else, it is vitally important that we better understand social media since it has become highly culturally relevant, a dominant form of communication and expression, a major media type used by companies for advertising and other forms of communication, and even has geopolitical ramifications.[4] Previous exploratory studies addressing teenagers discussed that advertising in the online social networking environment is not as successful as originally anticipated. The future success of online social networking sites as an advertising medium depends on its acceptance as an advertising vehicle that can deliver a message to a micro-target in a manner that will be well received and that increases the likelihood of interaction.[5] Technological developments create different effects on different generations. Young generation (high school/student age, 15 - 24) are specially interesting since, in this generation, social media promotes civil society and public opinion. The generation called digital natives is in contact with their families and friends from all over the world, can find a spouse or romantic relationship, can participate in civil protests, as well as can receive e-mail or online therapy support via social media.[6] Although generational approaches can be rightly critiqued as over-broad and dismissive of important racial, ethnic, national, and regional differences, and yet, we persist in finding utility in this shorthand. It is difficult to know whether the trends being captured will endure into adulthood, which is one of the reasons that generational studies mature along with the population.[7]

---

3 Barkhuus L; Tashiro J., *Student socialization in the age of Facebook*, in: Proceedings of the 28th International Conference on Human Factors in Computing Systems, ACM Press, New York, 2010, pp. 133–142.

4 Appel, G.; Grewal, L.; Hadi, R. et al, *The future of social media in marketing*, J. of the Acad. Mark. Sci., Vol. 48, 2020, pp. 79-95.

5 Kelly, L.; Kerr, G.; Drennan, J., Avoidance of Advertising in Social Networking Sites: The Teenage Perspective, Journal of Interactive Advertising, Vol. 10, No. 2, 2010, pp. 16-27.

6 Kahraman, A., *The relationship of generation Z with digital technology*, Uluslararası Anadolu Sosyal Bilimler Dergisi, Vol. 4, No. 2, 2020, pp. 113-134.

7 Rue, P., *Make Way, Millennials, Here Comes Gen Z*, About Campus, Vol. 23, No. 3, 2018, pp. 5-12.

3. RESEARCH OBJECTIVES AND METHODOLOGY APPROACH

Greater personalization typically increases service relevance and customer adoption, but paradoxically, it also may increase customers' sense of vulnerability and lower adoption rates.[8]

This paper aims to answer how 15 – 24 years old population in Croatia consumes media, content, and social media, to provide comprehensive view on Croatian youth by covering wide scope of topics related to values, perception, and behaviour of this target group, with an insight into their lifestyle and value system. The research was conducted in September 2022 in two phases. First phase was exploration through qualitative methodology: 4 focus groups (two 15 – 18 years old., two 19 – 24 years old), n=32, urban, 2 cities. Second phase was validation of collected insights through quantitative methodology: online survey, n=400, 15-24 years old, national representative sample of the target group. Descriptive statistics were used to provide an overview and foundation for further data analysis.

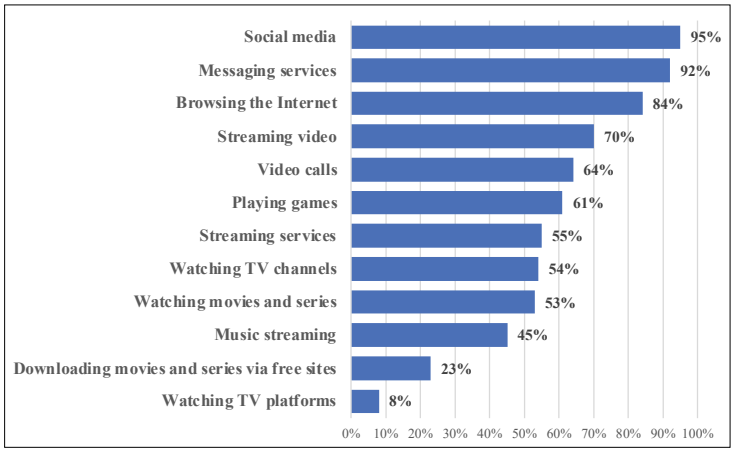
4. RESEARCH RESULTS

Qualitative phase gave an insight in fundamental life values of young generation. Focus groups results showed that They are eager to fully embrace and experience all that life has to offer, which is quite typical for this stage of life. Additionally, they hold close relationships with their loved ones and friends dear, and many still seek the support and guidance of their families and feeling rooted in their communities. Ability to stay true to oneself and be open about one's thoughts, beliefs, feelings, and identities is highly valued. It is also about honesty – there is a strong desire to see transparency in people, brands, and organizations. Authenticity builds trust. It fosters deeper relationships, as it encourages being open and vulnerable, so to be able to establish meaningful connections. Boundaries are blurred between fun, education, interests, hobbies, and work. There is no one profession, neither one career. There is not just graduating from school or faculty but creating a portfolio of skills. Hobby can become a source of successful business idea. Traveling is a school of life. They play active role in creating own personalized life path, based on exploration and flexibility. There is no one, formal, prescribed way. There is only "my way". Starting from creation of own curriculum to own business. Not following predetermined path along with flexibility is also their way to deal with unstable social and political context (unlike the older generations prone to stick to familiar and offered as solutions for insecurity). Young

[8] Aguirre, E.; Mahr, D.; Grewal, D.; Ruyter, K. D.; Wetzels, M., *Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness*, Journal of Retailing, Vol. 91, No. 1, 2015, pp. 34-59.

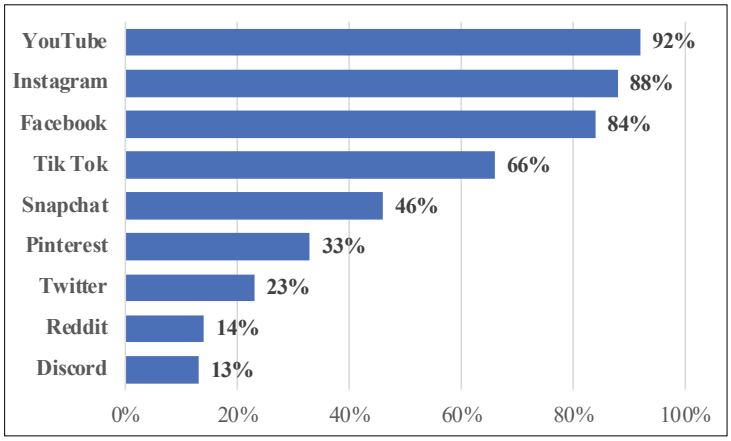
generation appreciate brands who get to know them and approach them with offers that address their specific needs and interests. Balance is the solution: work and life, technology and human contact, self-care, and care for the community. This generation is ambitious and strive for success, but not at the expense of well-being and leisure. Therefore, work-life balance is priority – it is their definition of success. It is imperative for them to find time for loved ones and self-care. Mental health issues caused by discrepancies between online and real world are becoming significantly more relevant. While technology can provide various benefits, it can also contribute to some well-being challenges. Excessive screen time, social media comparison, fake news is some of concerns. Embracing entrepreneurship over traditional employment is essential to overcome financial challenges, gain independence and even to become wealthy. They feel responsible to act regarding issues such as climate change and sustainability, inequality, community well-being. The same is expected from companies and brands. This generation has a strong desire to enhance society and the world at large, so brands that can associate themselves with positive change are more likely to attract them. Media for this generation is social media: social networks and browsing internet are the dominant activities of young generation (graph 1).

Graph 1. Which of the following services do you personally use at least once a week? Base: all respondents



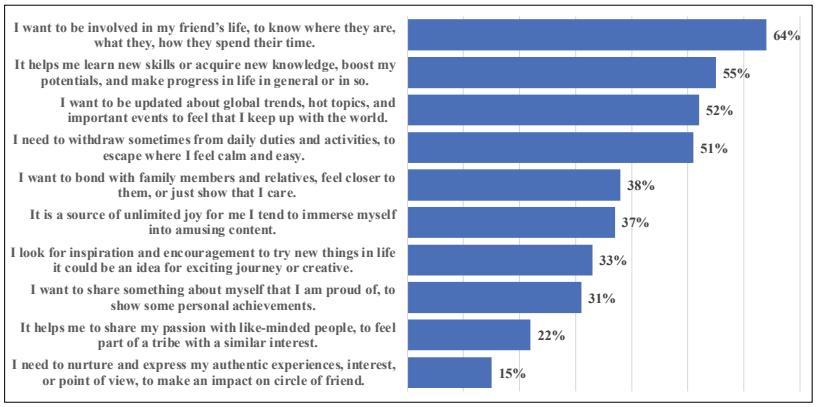
As presented in graph 2, YouTube, Instagram and Facebook are the most popular social networks, while Instagram is the most often used.

Graph 2. Which social networks do you use at least occasionally? Base: all respondents



Among social network users, Instagram is most often used by 38% of social network users which means that Instagram is the number one platform to be used for interaction with young generation. Though Facebook has been losing relevance and considered outdated (and for their parents), it should not be neglected. It still has some role – more for practical reasons/communities. Tik Tok is also important "place" where young generation spend a lot of their time (even they feel a bit addicted to it), but careful approach is needed. Social media has multiple usage purpose. In the first place, getting informed, learning, connecting, but escaping too. The use of social media is driven by the desire to be informed. Young Croatians perceives social media as necessary in their everyday life, although it causes serious concerns: sometimes they feel unproductive, guilty for overuse, and fearful of spreading negative content or fake news. They enjoy using it but also feel excessively dependent, distracted, and unable to imagine life without it. They're worried about its addictive nature and its potential impact on mental health and the pressure to maintain an online image. There is a need to control and limit the use, protect privacy, and balance it with non-digital activities. To understand the behaviour, it is important to know the motives for using the social media.

Graph 3. What people look for in social media.

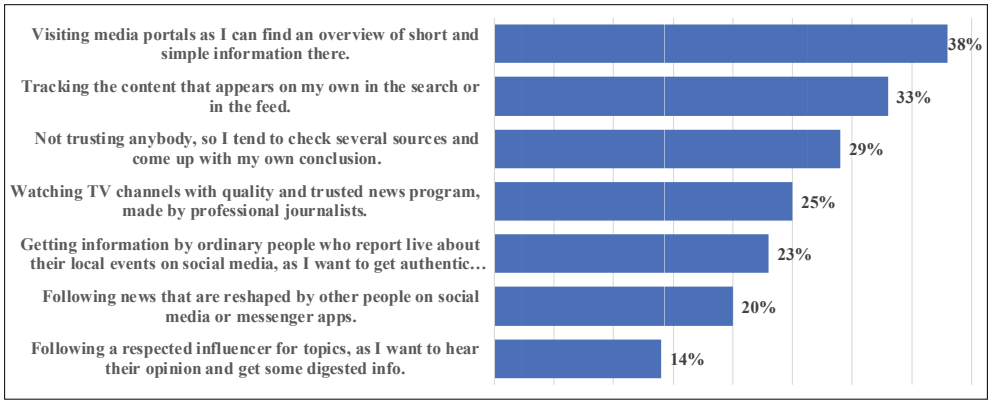


Since almost all needs are met on social networks, there are many opportunities how to utilize its power to engage successfully with young generation. Previous theorizing and research suggest that brand social networks engagement (beyond just basic "liking") may positively impact consumer attitudes and behaviours when members are induced to engage with them, exerting effort after joining.[9] Social media should be used for offering them opportunities for exploration, learning and socialization. Brands that leverage social media in an ethical and responsible way can differentiate themselves by taking on a supportive role. The young population is united by their interest in music. To attract young generation, focus should be on creating engaging and relevant content that aligns with generational trends and interests, with dose of exploration and fun involved. Music, travel, food, and sport are topics of high interest for the majority. Companies, universities, brands trying to capture young target attention should consider incorporating elements such as storytelling, humour, and interactivity to captivate their attention and provide a memorable experience. As for staying informed, checking several information sources is typical. TV news is still relevant, along with feeds and media portals. Young Croats prefer to visit media portals for information. Similar results can be found around the world: students mostly use smart phones, tablets, laptops. With these tools, it has been revealed that students perform activities such as listening to and downloading music, watching TV, watching, and downloading videos from the internet, browsing social networks, surfing the internet. The students stated that digital technologies make life easier, but they can affect life negatively when

[9] John, L. K.; Emrich, O.; Gupta, S.; Norton, M. I., *Does "liking" lead to loving? The impact of joining a brand's social network on marketing outcomes*, Journal of Marketing Research, Vol. 54, No. 1, 2017, pp. 144-155.

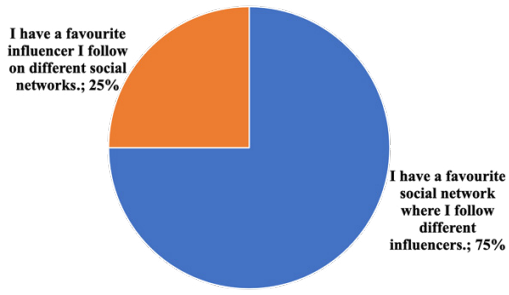
they are not used for the purpose and will lead to laziness, addiction and to blunt their imagination.[10]

Graph 4. Main ways to get informed



There is no one dominant way of consuming news. Young people tend to come up with their own point of view after checking several sources. Also, they prefer digested digital update, simple, short, and customised. In depth analysis of conducted focus groups or the young generation short, simple, visually striking doesn't mean superficial. They appreciate personal point of view – it gives value and credibility to news. These should be principles in content and format creation when trying to inform young generation. When it comes to their interest in influencers, the majority of analysed target group has a social network they prefer, where they follow different influencers. When asked to name up to three influencers that they like and follow, 254 names came up in total.

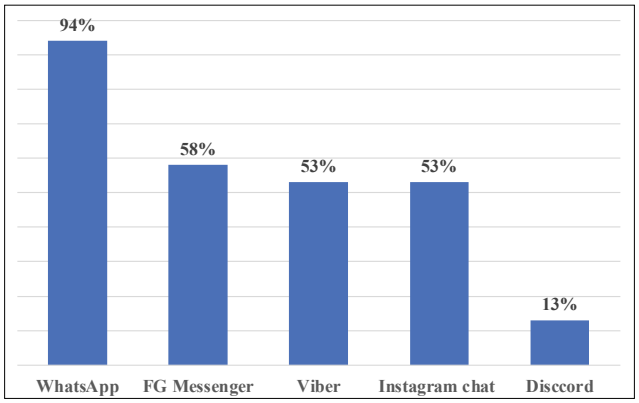
Graph 5. Favourite influencers and social networks



[10] Erten, P., *Z generation attitudes towards digital technology*, Gümüşhane University Journal of Social Sciences Electronics, Vol. 10, No. 1, 2019, pp. 190-202.

Focus groups insight analysis shows that authentic and inspirational is important: influencers who are seen as authentic, sharing personal experiences, relatable, and inspiring are favoured by young. They prefer influencers with a purpose, focusing on activism, positivity, open-mindedness, and humour beyond just popularity. Stories of real-life success and motivational content are highly valued. They also prefer local celebrities with authentic backgrounds. Nevertheless, controversial personalities gain attention and cause ambivalent feelings. Influencer marketing is worth investing in. However, selection of impactful and relevant influencers should be done with cautious. Question of authenticity is even more important for influencer appeal – honesty, genuine life stories, motivational narrative, but also purpose are some of the features. As for the usage of communication apps, young Croatians mostly use WhatsApp, although the number of multiple answers shows that the majority use multiple applications.

Graph 6. Used communication applications.



5. DISCUSSION

Earlier research on social media within young generation argued that active usage of social media platform has already changed the virtual bazaar, the place of work and the society; this will gradually pave way to develop innovative commerce models, products, and techniques. However, some questions are there concerning how young generation and their use of social media will shape individual, organizations and societal outcomes in different situations.[11] Our research confirmed that media for 15-24 generation is social media: social networks (95%), messaging services (92%) and browsing internet (84%) are the dominant activities of young generation. YouTube (92%), Instagram (88%) and Facebook (84%) are the most

[11] Prakash Yadav, G.; Rai, J., *The Generation Z and their Social Media Usage: A Review and a Research Outline*, Global Journal of Enterprise Information System, Vol. 9, No. 2, 2020, pp. 110-116.

popular social networks, while Instagram is the most often used (38%) which means that Instagram is the number one platform to be used for interaction with young generation. Though Facebook has been losing relevance and considered outdated (and for their parents), it should not be neglected. It still has some role – more for practical reasons/communities. There is no one dominant way of consuming news. Young people tend to come up with their own point of view after checking several sources, which is important for positive impact in terms of digital media use and youth. Other research confirmed that the positive impacts depend on directly political uses of digital media, such as blogging, reading online news, and online political discussion. These online activities have off-line consequences on participation, such as contacting officials, talking politics, volunteering, and protesting.[12] When analysing how young population in Croatia consumes content, based on focus groups insights there are several principals in content creation: authenticity, customization, and interactivity. Almost all their needs are met on social networks. Content they prefer should offers multidimensional and multisensorial experiences, encouragement, and inspiration. When thinking strategy, elements such as storytelling, humour, and interactivity should be integrated to captivate their attention and provide a memorable experience. Personal, subjective experiences, points of view and life stories are engaging and credible. Focus groups insight analysis also show that they prefer influencers with a purpose, focusing on activism, positivity, open-mindedness, and humour beyond just popularity. As for the usage of communication apps, young Croatians mostly use WhatsApp, although the number of multiple answers shows that the majority use multiple applications. The way they use media, social network, and create/consume content changes daily, so legal framework should follow.

6. CONCLUSION

Change in the media landscape is constant. Young people are growing up in a completely new digital environment. Complexity of creating communication strategies and media channels optimization when communicating with young people and speed of change in technology, communication channels and ways of creating and consuming content requires up-to-date knowledge about motives, preferences, and behaviour, followed by relevant legal frameworks. Therefore, understanding values, perception, and behaviour of youth when it comes to social media is ground zero for further analysis. Since this paper is based on descriptive statistics there are some limitations in interpretation, primary that there is no in-

[12] Boulianne, S.; Theocharis, Y., *Young People, Digital Media, and Engagement: A Meta-Analysis of Research*, Social Science Computer Review, Vol. 38, No. 2, 2020, pp. 111-127.

formation on relationships, causes, or effects of analysed data, which should be the focus of further research on this topic.

REFERENCES

BOOKS AND ARTICLES

1. Aguirre, E.; Mahr, D.; Grewal, D.; Ruyter, K. D.; Wetzels, M., *Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness*, Journal of Retailing, Vol. 91, No. 1, 2015, pp. 34-59
2. Aichner, T.; Grünfelder, M.; Oswin Maurer, O.; Jegeni, D., *Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019*, Cyberpsychology, Behavior, and Social Networking, Vol. 24, No. 4., 2021, pp. 215-222
3. Appel, G.; Grewal, L.; Hadi, R. et al, *The future of social media in marketing*, J. of the Acad. Mark. Sci., Vol. 48, 2020, pp. 79-95
4. Barkhuus L; Tashiro J., *Student socialization in the age of Facebook*, in: Proceedings of the 28th International Conference on Human Factors in Computing Systems, ACM Press, New York, 2010, pp. 133–142
5. Boulianne, S.; Theocharis, Y., *Young People, Digital Media, and Engagement: A Meta-Analysis of Research*, Social Science Computer Review, Vol. 38, No. 2, 2020, pp. 111-127
6. Erten, P., *Z generation attitudes towards digital technology*, Gümüşhane University Journal of Social Sciences Electronics, Vol. 10, No. 1, 2019, pp. 190-202
7. John, L. K.; Emrich, O.; Gupta, S.; Norton, M. I., *Does "liking" lead to loving? The impact of joining a brand's social network on marketing outcomes*, Journal of Marketing Research, Vol. 54, No. 1, 2017, pp. 144-155
8. Kahraman, A., *The relationship of generation Z with digital technology*, Uluslararası Anadolu Sosyal Bilimler Dergisi, Vol. 4, No. 2, 2020, pp. 113-134
9. Kelly, L.; Kerr, G.; Drennan, J., *Avoidance of Advertising in Social Networking Sites: The Teenage Perspective*, Journal of Interactive Advertising, Vol. 10, No. 2, 2010, pp. 16-27
10. Prakash Yadav, G.; Rai, J., *The Generation Z and their Social Media Usage: A Review and a Research Outline*, Global Journal of Enterprise Information System, Vol. 9, No. 2, 2020, pp. 110-116
11. Rue, P., *Make Way, Millennials, Here Comes Gen Z*, About Campus, Vol. 23, No. 3, 2018, pp. 5-12

WEBSITE REFERENCES

1. Ortiz-Ospina, E., *The rise of social media*, Our World in Data, 2019, [https://ourworldindata.org/rise-of-social-media], Accessed 10 June 2023

UDK 37.091.33-028.27:34
Original scientific paper

SUPPORTING LAW TEACHERS' IN THE DEVELOPMENT OF MOOCS*

Sandra Kučina Softić, PhD, Assistant Professor
University of Zagreb, University Computing Centre
Josipa Marohnića 5, 10 000 Zagreb, Croatia
sskucina@srce.hr

Tea Čičko
University of Zagreb, University Computing Centre
Josipa Marohnića 5, 10 000 Zagreb, Croatia
tea.cicko@srce.hr

Petra Kvočić
University of Zagreb, University Computing Centre
Josipa Marohnića 5, 10 000 Zagreb, Croatia
petra.kvocic@srce.hr

Tona Radobolja
University of Zagreb, University Computing Centre
Josipa Marohnića 5, 10 000 Zagreb, Croatia
tona.radobolja@srce.hr

ABSTRACT

Modernising law and legal education are inevitable in today's society. Possible arguments for not taking such steps disappeared with the pandemic which fostered processes which were postponed or were found as not applicable. Onwards, the COVID-19 pandemic has further accelerated the existing trend toward online and hybrid learning. It uncovered new and innovative ways for students and educators to organise their teaching and learning activities and to interact in a more personal and flexible manner online. Several papers and policies on the European level, among them Digital Education Action Plan highlight the importance of developing a high-performing digital education ecosystem and higher levels of digital capacity

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

of education and training systems and institutions. Still, the process of modernisation and digitalisation of law and legal education is complex and requires significant efforts and resources from all stakeholders involved. The important aspect in this process is teachers' preparedness and ability to implement digital technologies in teaching and learning, the support they need in this process as well as their training in digital skills to be able to properly use and implement digital technologies using new teaching methods and digital pedagogies. This paper discusses how to support teachers in the digitalisation of law and legal education and teachers' training in acquiring necessary digital competences. This is part of the Erasmus+ project Digital in Law Education (DIGinLaw) where one of the results is the development of 12 MOOCs on the topic of law and legal education in higher education. The aim of this paper is to reveal the significance of organizational support for teachers and the importance of developing teachers' digital skills and competences for successfully meeting the challenges of the digitalization of legal education. The paper describes the process taken to support teachers in the development of MOOCs including their training in digital skills. The results of the research – the proposed model of supporting and training teachers in MOOC design - can be applied to similar requirements for higher education teachers' support in implementing digital technologies in teaching and learning. Using the survey as a quantitative research method and in-depth semi-structured interviews as a qualitative method, the paper gives insight into teachers' readiness to use digital technologies and what kind of support and training they need to sufficiently implement digital technologies in the educational process.

***Keywords**: digital technologies, MOOC, digitally competent teachers, organized support, teachers' training, digitalisation, legal education*

1. INTRODUCTION

Digital transformation today is no longer a matter of choice - it is inevitable, necessary and unavoidable. It refers to the process that starts from the moment when the organization starts to think about the introduction of digital technologies in all areas of business and lasts until the moment of their complete integration.

Today, after the crisis caused by the COVID-19 disease pandemic and everything we have been through, it is clear that we have already taken a deep step into digital transformation, but it is important that to try to put everything together systematically, plan strategically and realize it. Digital transformation has become one of the key strategic goals of the development strategy of most higher education institutions. Onwards, the COVID-19 pandemic has further accelerated the existing trend toward online and hybrid learning. Horizons have been broadened and the consequences have begun to be dealt with, which must be faced, but also anticipated and invested in the time that is coming and which must no longer surprise us. It is important to encourage a digital culture that fosters innovation and entrepreneurship and to develop the institution's digital strategy. In addition, it is extremely important to ensure the continuous professional training of teachers so that they have digital competences for the introduction of new teaching methods, for the transition to a model in which the student's educational process

is at the centre and so that they can ensure that students acquire the competences that are needed today and tomorrow, for jobs that don't even exist yet, as well as being able to fully participate in the society of the digital age. Increased digitalization has changed the way legal services are conducted. Future lawyers ought to be competent and skilled to meet the needs of their clients, law firms and the court system. The partners of the DIGinLaw project acknowledge that the lack of specific methodology in an e-course creation and performance caused by insufficient digital competences of the HE lecturers may impede the full capacity of legal knowledge transfer in a virtual environment. Thereby, the project supports the training of educators as well as raises awareness of its significance for HE of the future in general. The process of modernisation and digitalisation of law and legal education is complex and requires significant efforts and resources from all stakeholders involved. Setting MOOCs on topics in the field of digitalization of law (cross-border dispute resolution in the digital age, consumer protection in the digital age, artificial intelligence, cryptocurrencies in international private law, etc. is one of the possibilities digital technologies bring. Online learning makes it possible for learners to take up a course without attending an educational institution. Learners get the benefit of taking up a course from their home or from any place they're comfortable. It also enables learners to get credible certifications, thereby, improving their qualifications, which, in turn, play an important role in career progression.[1] [2] MOOCs also represent a kind of novelty in the context of thematic content but also teaching methodology in higher education in the field of law.

1.1. The DIGinLaw project

The Erasmus+ project Time to Become Digital in Law - DIGinLaw [3] is a consortium of higher education institutions aware of how strongly digitalization affects society, science and the transfer of knowledge. While taking advantage of modern technologies at low environmental costs, the DIGinLaw project aims to raise awareness of digital demands in HE in law and fosters the creation of digital literacy and digital competence that is needed in the law labour market. It also aims to foster the free circulation of highly educated workers and create an open and inclusive society of legal knowledge and open access to the scientific area dealing with the effects of digitalization on law and legal education. This Erasmus+ project

1 European Commission, *European Universities Initiative Survey on the impact of COVID-19 on European Universities,* 2020, [https://erasmus-plus.ec.europa.eu/document/coronavirus-european-universities-initiative-impact-survey-results], Accessed 10 February 2023.

2 WEF, *The future of jobs*, 2020, [https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf], Accessed 10 February 2023.

3 DIGinLaw project web page, [https://www.pravos.unios.hr/diginlaw/], Accessed 8 February 2023.

is coordinated by the Faculty of Law at the University of Osijek, Croatia and partners on the project are The University Court of the University of Aberdeen, UK, Universita degli Studi di Milano, Italy and the University of Zagreb University Computing Centre SRCE, Croatia.

The overall objective of the DIGinLaw project is to advance the utilization of digital technologies in higher education in law. One of the objectives of the project is to contribute to building and advancing the performance of online higher education teaching in law studies. This specific objective is assured by providing quality training on digital competences addressed to law professors and lecturers. Training would develop the digital competences of HE law teachers and lecturers at three law faculties involved and result in an advanced level of performance of online HE teaching in law. SRCE as the project partner has focused its expertise on this objective.

2. THE THEORETICAL BACKGROUND

2.1. The E-learning Centre at SRCE

The University of Zagreb University Computing Centre (SRCE) [4] is the oldest infrastructural institution of the academic and research community in the area of the application of information and communication technologies (ICT) in Croatia. SRCE is the key institution in planning, designing, constructing, and maintenance of the computing, data and information infrastructure, the e-infrastructure for the Croatian academic and research community. Furthermore, SRCE is the competence centre for information and communication technologies as well as the centre for education and support in the area of ICT application.

The focus of the E-learning Centre at SRCE (ELC) [5] is to provide accessible and sustainable support to higher education institutions, teachers and students in the use and application of new technologies in teaching and learning. The ELC is ensuring and provides a generally accessible e-learning platform and ensures joint/centralized resources required for the application of e-learning and finally, but not less importantly, the promotion and dissemination of information about e-learning.

The ELC supports users in the process of the implementation of e-learning technologies in the educational process. The team provides help to teachers in the

[4] University Computing Centre University of Zagreb. [https://www.srce.hr], Accessed 8 February 2023.

[5] E-learning Centre at the University Computing Centre University of Zagreb, [https://www.srce.hr/elc], Accessed 8 February 2023.

preparation and maintenance of e-courses (blended mode or fully online), organizes training for teaching staff in e-learning technologies and course design and supports students in the virtual environment.

The Centre is providing everyday support via the helpdesk (phone, e-mail) and consultations with teachers. In addition, there are numerous learning materials like manuals, animations, quick help, guidelines and frequently asked questions that enable users to find information in the way that best suits them. The ELC has also prepared a number of training courses and workshops for teachers. Moreover, the ELC team holds daily consultations with teachers, devoting themselves to each individual teacher and his/her e-course. Creating a positive and creative environment, informing about e-learning and its possibilities in the academic community and providing quality and systematic support to users are long-term goals of the E-learning Centre at SRCE.

Therefore, the role of the SRCE E-learning Centre in this project was to provide training for teachers and support them in the design and development of MOOCs (Massive Open Online Courses). Therefore, SRCE developed the online course titled Digital Competences of HE Teachers for Innovative Teaching Practices and organized teachers' training that will enable them to create high-standard e-learning courses in law - MOOCs. Afterwards, the ELC team provided support to teachers in the development of MOOCs and in the end the evaluation of the developed MOOCs with recommendations for their improvement.

2.2. Supporting teachers in enhanced teaching and learning

Digital technologies have become ubiquitous in all aspects of life, work and learning. [6] Today, we can hardly imagine life without the use of mobile phones and computers, we primarily search for information on the Internet, and very often, we learn by attending online courses, reading various materials and watching tutorials and animations available on the Internet. However, in the formal education system, teaching still takes place dominantly in the classroom without the use of digital technologies, or they are used only as an addition to the teaching and for the preparation of lessons.[7] Nevertheless, the use of e-learning and digital technologies in education has been present for a long time, and many teachers and educational institutions try to implement them into the educational

[6] Bates, A.W., *Teaching in a Digital Age – Third Edition*, Tony Bates Associates Ltd., Vancouver, B.C., 2021.

[7] Brooks, D.C.; McCormac, M., *EDUCAUSE: Driving Digital Transformation in Higher Education* ECAR research report, ECAR, Luisville, 2020.

process on a smaller or on larger scale. Implementation and use of digital technologies in teaching and learning in higher education have become unavoidable in modern education, primarily because of the opportunities and advantages this technology brings to education as well as its role in enabling the achievement of educational goals.[8] After two years of a pandemic that moved education online, we have different views, attitudes and experiences with digital technologies than before. The picture is more nuanced than before, as surely teachers and educational institutions will keep on using some of the digital technologies they found most effective for the educational process. However, with the increasing number of various tools and technologies, the teacher very often loses pace because he/she cannot follow the news so quickly, familiarize himself/herself with them and find the right way to integrate them into the educational process.[9] [10] Therefore, organizational support for teachers is one of the most important factors. Such organisational units follow trends and enable teachers to implement innovative technologies and tools in teaching beyond the standard. They offer regular and varied training courses to teachers and work continuously on the further development of digital learning tools.[11] The importance of organizational support to teachers in the use and implementation of digital technologies was confirmed during the pandemic, clearly indicating the importance of e-learning centres, as central specialized units to provide support to teachers and education institutions within the system. For example, the Lotus report titled National Developments in Learning and Teaching in Europe states that such centres can serve as instrumental in providing support and advising on the use of technology and pedagogy related to digitalisation, and serving as coordinators for the exchange of good practices between teachers.[12] Last, but not least, the pandemic experience learned us all how to seek help and acknowledge we need it.

---

8 Brown, M., *What are the Main Trends in Online Learning? A Helicopter View of Possible Futures,* Asian Journal of Distance Education, Vol. 16, No. 2, 2022.

9 Kučina Softić, S.; Radobolja, T; Martinović, Z., *How did we support education in pandemic- role of the e-learning centre*, EDEN Digital Learning Europe Proceedings, 2022 Annual Conference Tallinn, 20-22 June 2022.

10 Brown M.; Connole G.; Beblavy, M., *Education outcomes enhanced by the use of digital technology: Re-imagining the school learning ecology*, EENEE Analytical Report No. 38, Luxemburg, 2019.

11 European Commission, *European Education and Training Expert Panel: Summary of findings and of the discussions at the 2019 Forum on the Future of Learning*, Luxemburg, 2019, [https://op.europa.eu/en/publication-detail/-/publication/b976dfa7-a6a9-11e9-9d01-01aa75ed71a1/language-en], Accessed 10 December 2022.

12 Zhang, T., *National Developments in Learning and Teaching in Europe*, European University Association, Brussels, 2022.

2.3. Teachers' training in digital competences for innovative teaching practice

New technologies bring new opportunities for teaching and learning, and in addition to being an expert in the subject field, the teacher needs to monitor the development of ICT and be acquainted with them as well as have good pedagogical background to know how to implement them in the educational process. [13] [14] The teacher is facing a great challenge; he/she is expected to be competent in using new technologies, to be able to apply them in the educational process and to introduce new teaching methods. There is increasing pressure on the teacher who is expected to have all the necessary knowledge, but no one asks whether they have it, what are the conditions in which they work when it comes to teaching and how they will acquire the necessary knowledge and competencies to fulfil all the expectations. New Digital Action Plan 2021-2027 adopted by European Commission[15] defines the enhancement of digital skills and competences for digital transformation as the strategic priority. The Action Plan also stresses the importance of training in digital skills including digital teaching methods of teachers. Therefore, teachers and educators should be empowered to adopt innovative methods.

The pandemic also enhanced the use of digital technologies, as with the lockdown and closing of campuses and physical premises of higher education institutions, teaching and learning had to move to the online environment. For many HE institutions and teachers, this was the first experience with the use of digital technologies at all or in an extensive way. During the pandemic, teachers gained significant experience in the use of digital technologies. Some are good and some are poor because of a lack of digital competences and knowledge of how to integrate them into the educational process. Also, quite often teaching and learning in the online environment during the pandemic was misused for online education, but it was mostly emergency remote teaching where traditional classroom teaching was just transferred to an online environment.[16] Nevertheless, the gained experience is

---

13 Kučina Softić, S.; Odak, M.; Lasić Lazić, J., *Digitalna transformacija: Novi pristupi i izazovi u obrazovanju*, Sveučilište Sjever, Koprivnica, 2021.

14 Gaebel, M.; Zhang, T.; Stoeber, H. & M. A., *Digitally enhanced learning and teaching in European higher education institutions,* European University Association, Brussels, 2021.

15 European Commission, *Digital Education Action Plan 2021-2027: Resetting Education for Digital Age*, European Commission, Brussels, 2020, [https://education.ec.europa.eu/focus-topics/digital-education/action-plan], Accessed 10 December 2022.

16 Bond, M.; Bedenlier, S.; Marín, V.I. *et al., Emergency remote teaching in higher education: mapping the first global online semester,* Int J Educ Technol High Educ, Vol. 18, 50, 2021.

important to plan the education process not only for today but for the future as well and to adapt it to the digital age.[17] [18]

It is very difficult for teachers to expect to be innovative or teach differently from the *historical model* (the teacher is at the centre of the education process and conveys knowledge to students) unless they understand other possible ways of teaching based on theory and research. Teachers should be encouraged to think outside the box and not just use technology to replicate conditions in the classroom but instead think about how technology can be used to improve learning and "do stuff that you can't do in the classroom". Especially after emergency remote teaching prevailed in the pandemic, teachers have to be aware that it was a temporary situation and that move to online teaching and learning was not planned and designed initially for such form. Lessons learned enabled teachers and educators to gain a deeper understanding of the possibilities that digital technologies can bring to education and online education as such. It also enlightened them that moving online should be discussed and prepared more seriously, not leaving it solely to teachers to cope with it. Without organized and systematic support to teachers, they will be less eager and interested to use and implement digital technologies in the educational process, and what is even worse, they will develop a distorted image of online education, either fully online or as a hybrid mode with a large online component.

Therefore, the project intellectual output O1 has focused on the building and advancement of digital competences of higher education teachers. So, one of the first tasks is the project were to develop a training program for teachers which consisted of e-course and designed training activities. The first step was to identify participants (teachers) who will attend the training and their experience in the use of digital technologies, as well as how much do they know about MOOCs. This was done during online project meetings with project partner representatives. SRCE developed an online course titled "Digital competences of HE teachers for innovative teaching practices" which is available on the e-learning platform MoD (mod.srce.hr). The aim of the course was to raise awareness of the importance of teachers' digital competences and continuous professional development that will enable them to implement digital technologies in a proper way into teaching and learning, to provide them with guidelines on how to do it and to introduce to

---

17 Župan, M., *Online Legal Education in Croatia*, in: Nottage, L.; Ibusuki, M. (eds.), Comparing Online Legal Education, Intersentia, Cambridge, 2022.

18 Kumi-Yeboah, A.; Sallar, A.W.; Kiramba, L.K.; Kim., Y., *Exploring the use of digital technologies from the perspective of diverse learners in online learning environments,* Online Learning, Vol. 24, No. 4, 2020, pp. 42-63.

them Moodle as the e-learning platform. The developed course consists of five modules and its duration is 20 hours.

Figure 1: Main page of the training course for teachers "Digital competences of HE teachers for innovative teaching practices"

Source: https://mod.srce.hr/course/view.php?id=391

In July 2021, SRCE organized training for teachers from partner institutions. Due to the pandemic, training was organized online and lasted three days. The aim of the training was to increase the digital competences of teachers from the project partners' institutions and prepare them for the development of MOOCs. One of the activities within the training was taking the tutor-led course "Digital competences of HE teachers for innovative teaching practices". During and after training teachers had assignments that they had to fulfil and which were evaluated. They were mandatory in order to receive the certificate and digital badge that they have finished the course. Upon finishing the training, teachers had the possibility for online consultation with the SRCE team. After the training, the course was adapted to be self-paced and is open to everyone.

2.3.1. Participants' feedback on the training

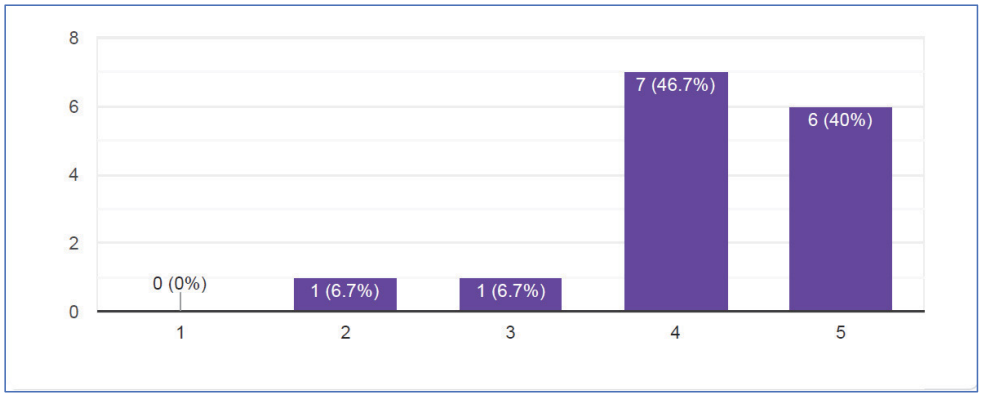
Fifteen participants took the training and provided their feedback in a survey prepared by the project coordinator. Quantitative research based on a survey was prepared. Likert scale was used in questions, with a scale from 1 to 5 with 5 as the highest and 1 as the lowest grade.

Based on the feedback, participants are satisfied with the training and it has reached its goal. Participants graded clearness of the objectives of the event, with an equal percentage of (46, 7%) for grade 4 and for grade 5, in total 93,4%. In addition, 86, 7 % of participants said that the objectives of the event have been met rating them with a grade of 4 or 5. The same percentage (86, 7%) was received in the question on how was the information during training presented as well as on the question on the clearness of the support materials prepared for the training.

Participants indicated that the training improved:

- their knowledge - 66,7% of them gave the grade 5 and 33,3% gave the grade 4;
- their digital skills – 53,3% gave a grade of 5, 26,7% gave a grade of 4 and 20% gave a grade 3
- their pedagogical and methodological skills – 40% gave a grade of 5, 46,7% gave a grade of 4 and 13,3% gave a grade of 3

Figure 2: Answers to the question "What is your overall evaluation of the training?" (Scale from 1 to 5 with 5 as the highest and 1 as the lowest grade)



Source: Author's research

The majority of participants (86, 7%) evaluated the training with grades 4 and 5, which indicates that the training reached its goal.

2.4. Supporting teachers in MOOC development

During MOOC development, teachers had the continuous support of the SRCE ELC team.

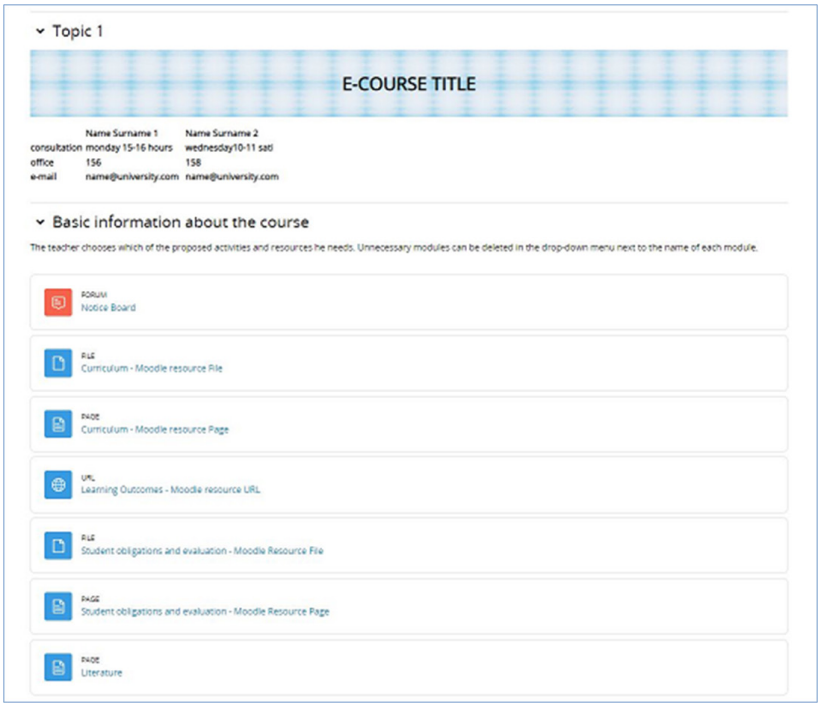
The support was organized through:

- continuous consultations
- designed Course Development Form
- designed Template for MOOC design
- opening of the e-course for MOOC development, enrolment of teachers
- evaluation of the developed MOOC with recommendations for improvement.

In the Course Development Form, teachers will describe the aim of the course and how it will be organized and the ELC team provided feedback on it as well. This helped teachers in the preparation of the MOOC design.

The ELC team prepared a Template for the MOOC design, which can be integrated into an empty online environment to help teachers to start with MOOC development.

Figure 3: Template for MOOC design



MOOCs are developed on the e-learning platform based on Moodle (mod.srce.hr) which is maintained by the ELC team. Therefore, the ELC team provided support in the opening of the MOOCs, enrolling the teachers into the course and in technical details related to the use of Moodle. Support was also provided on the design of the MOOC based on the course development forms. The ELC organized as well several group consultations on a defined topic.

During the process of the MOOC development, the ELC team provided support and help when needed. Upon finalisation of their MOOC, teachers reported it to the ELC team who then made an evaluation and provided feedback. Feedback consisted of technical parts related to the proper use of resources and activities in Moodle, but also on MOOC design- choice of the teaching methods, how the digital learning materials have been presented, defined learning outcomes and assessment. When teachers improved their MOOCs, the SRCE team provided a second round of feedback.

3. METHODOLOGY, RESULTS AND DISCUSSION

3.1. Research method

SRCE team conducted in September 2022 qualitative research with teachers from partner institutions who are developing MOOCs, with the aim to get their feedback on the experience of the MOOCs preparation and development. This research is built on the work done in IO1 in the project and relates on the overall topic of digitalization of legal education and digitalization of law. In parallel with the research, the SRCE team evaluated the developed MOOCs.

The research was conducted in the following way:

- literature review
- short introductory survey
- interview with teachers from partner institutions (main method)

As a research method, qualitative research was used with semi-structured interviews.[19] [20] Each interview consisted of two parts; the first part was a short survey with questions and the second part semi-structured interview. In addition, the SRCE team did a literature review related to teaching and learning during the pandemic. The received feedback will enable the SRCE team to fine-tune the

[19] Creswell, J. W., *Research design: Qualitative, quantitative, and mixed methods approaches*, 2nd ed., Sage, 2011.

[20] Merriam, S. B., *Qualitative Research: A Guide to Design and Implementation,* Jossey-Bass, 2009.

designed training of teachers and support so it can be used as a model for similar scenarios.

Research hypotheses are:

- Training and support provided to teachers by the SRCE ELC team were enough for teachers to be able to design their first MOOC
- Based on gained experience in the development of the first MOOC, teachers are more open to using digital technologies in their teaching.

The first part of the research was a short survey consisting of questions related to the demographic part and teachers' digital competences and consisted of seven questions.

The second part was a semi-structured interview starting with the context and the profile of participants and then questions related to the following issues. The 17 questions in total:

- [Attitudes] to identify and analyse what participants think about the implementation of e-learning in the educational process and how they feel about MOOCs.
  - What is your attitude towards the use of e-learning in Law subjects?
  - Have you yourself attended any MOOC? If yes, how do you find it? If not, why not?
  - What is your attitude towards developing MOOC in the DIGinLaw project? How did you perceive this task (easy, difficult, unrealistic...)?

- [Adaptability] To identify and analyse the kind of adjustments and the degree of flexibility teachers need to adapt to new circumstances and work in an online environment, especially those teachers who had no prior experience in e-learning and MOOCs.
  - How did you prepare for the development of the MOOC?
  - Was your previous experience in teaching and use of digital technologies enough to start with the preparation and development of MOOC?
  - How much did you rely on support in the preparation of MOOC? What kind of support did you need? Technical, in learning design, in video preparation, pedagogical....
  - How did you prepare learning materials for MOOC? used existing ones, adapted existing ones or prepared new ones

- [Advantages and disadvantages] To identify and analyse the reasons expressed by teachers in the case they foresee further use (or not) of e-learning and available support.
    - Based on your experience in the use of digital technologies and e-learning so far, what would you identify as advantages and as disadvantages?
    - Now when you have developed MOOC, what advantages/disadvantages do you see in such a way of teaching? Would you copy this experience and way of teaching and learning to other courses?
    - Do you find your digital skills enough for the preparation of MOOCs and e-courses? Do you think that teachers' professional development in digital skills should be compulsory?
    - How important is support to teachers in the use of e-learning and new teaching methods? How should it be organized?
    - Would you recommend the use of e-learning and the development of MOOCs to other colleagues?

The target group of research are teachers who participated in the training organized by SRCE and are developing MOOCs within the DIGinLaw project. Six teachers participated in the research. They were from the University of Osijek (3 teachers), the University of Milan (2 teachers) and the University of Aberdeen (1 teacher).

Interviews were conducted online using SRCE videoconferencing system and recorded. Interviews lasted up to one hour. Before the interview, participants gave consent for participation in the research and for the recording of the interviews. The interviewee and interviewer signed the consent. The data were collected and analysed by the authors of the research and were stored on the SRCE server. Only authorized persons in SRCE have access to data. All received data during the interview were anonymised in the analysis and presentation of research results.

The obtained data (quantitative and qualitative (narrative analysis)) were tabulated in a Microsoft Excel (MS Excel) file. The processing of the data obtained from the research was carried out using MS Excel software.

3.2. Research results

Participants were five females and one male in the range of 31 to 60 years of age. Five of them have been teaching for more than 11 years and one for up to 10 years.

Teachers participating in the research already had some experience with online teaching and learning, which was gained mostly during the pandemic time and was mostly in the use of videoconferencing systems. None of the participants had experience with the development of MOOC before. The design of the MOOC in the DIGinLaw project was the first MOOC they were developing. Some of the teachers had knowledge of what MOOCs look like as they have attended some.

In a question about how they assess their digital competences for teaching in higher education one participant graded himself A2, two of them graded themselves B1 and three B2 on a scale from A1 to C2 with A1 being the lowest and C2 the highest level (Table 1). Levels A1 and A2 refer to the beginning of the use of technology in some areas and awareness of its potential in improving pedagogical and professional practice. Levels B1 and B2 refer to the application of digital technologies in different contexts and in different ways.

Table 1: Teachers' self-assessment of digital competences for teaching in higher education

	Levels					
Participants	A1	A2	B1	B2	C1	C2
P1		X				
P2			X			
P3				X		
P4			X			
P5				X		
P6				X		

Source: Authors research

Half of the participants (n=3) stated that they are quite sure about which e-learning tools and technologies to use in class, while others state that they use some e-learning tools and technologies for teaching, but are not sure how to choose the most appropriate ones. Four participants in this research stated that they have very good and good knowledge of the application of e-learning technologies, but two of them stated that their knowledge about the application of e-learning technologies is poor.

In the survey on higher education teachers and the pandemic of COVID-19 done by the Agency for Science and Higher Education, University Computing Centre and University of Rijeka in 2021, the results are very similar.[21] Research results showed that 87% of teachers find themselves to have good or very good knowl-

[21] Agencija za znanost i visoko obrazovanje, Sveučilišni računski centar Sveučilišta u Zagrebu, Sveučilište u Rijeci, *Visokoškolski nastavnici i pandemija: akademski i pshiološki izazovi*, Zagreb, 2021.

edge of the application of e-learning technologies. Taking into relation research results by Kučina Softić [22] where 69, 3% of teachers at the beginning of 2020 considered themselves to have good and very good knowledge of the ICT and e-learning application; the percentage in 2021 is higher and can be explained by teachers' gained experience during the pandemic. Looking into the research results done in higher education in Montenegro in 2021 [23] it can be seen that teachers' digital literacy significantly influenced the success of their online teaching ability during the pandemic. A similar conclusion can be reached in the research conducted at the University North [24], which shows that teachers who find themselves to have good knowledge of e-learning application in the educational process are more eager to have an e-learning component in their courses going to the hybrid model or fully online as well.

In the qualitative part of the interview, participants answered the following questions related to the context and profile of participants:

1. *Did you use digital technologies in your teaching during the pandemic? Which technologies did you use?*

All teachers used digital technologies in their teaching during the pandemic. The most used technologies are MS Teams and Zoom, PowerPoint presentations and e-learning platforms Moodle and Blackboard.

2. *Did you stream live your lectures during pandemic to reproduce face-to-face classroom lectures? Did you change anything in preparation or delivery of lectures online besides that they were now online?*

During the pandemic, the four participants (P1, P2, P4, P5) organized their lectures online using video conferencing tools. Most of them (P1, P4, P5) realised that during online lectures, it is important to engage the students, and they began to include group work and other tasks that required students' active participation in online lectures. Some teachers (P2, P3) developed learning materials for an online environment and some (P6) prepared short podcasts.

---

22 Kučina Softić, S., *Digitalne kompetencije nastavnika za primjenu e-učenja u visokom obrazovanju*, Zagreb, 2020, doctoral thesis.

23 Kavarić, M.; Kavarić, A.; Djokovic, R., *Challenges in online teaching during COVID-19 pandemic: Higher education survey in Montenegro*, Innovations in Education and Teaching International, 2021.

24 Kučina Softić, S.; Lasić Lazić, J.; Tropša, V., *Analiza ankete o stavu nastavnika prema tehnologijama e-učenja u visokom obrazovanju te koje digitalne kompetencije su im potrebne kako bi na kvalitetan način primijenili e-učenje u obrazovnom procesu*, Sveučilište Sjever, Koprivnica, 2022.

One participant (P3) explained how he/she had to change teaching method in an online environment after realizing that the traditional form of teaching was not adequate in an online environment:

„I live streamed and I had combination; so some of my lectures were like classic lectures in the beginning, but later on I had a combination with Moodle. And I was then creating different materials for students so they can learn on their own or follow up on my lectures. So, I started changing the teaching methodology. But at first, I was just speaking to the camera for three hours."

3. *How did you find out which digital technologies to use and did you have any support in learning how to use them?*

When the pandemic started, most of the participants (n=4; P1, P4, P5, P6) received a list of recommended technologies for online teaching and learning at their institutions. Some of them also had support from the University's IT department and had organized training in the use of digital technologies. One participant taught himself/herself how to use the recommended technologies, and two participants researched on their own which technologies would be adequate to use in class, with some help from their colleagues. After his/her own research, one participant subsequently received instructions from the university as well as provided professional assistance.

4. *Do you have an e-course today? Is this an addition to classroom teaching or do you use a hybrid model or a fully online one?*

Half of the participants (n=3) in the research have an e-course today in the hybrid form, while others do not have an e-course nevertheless they designed the MOOC.

Attitudes

1. *What is your attitude towards the use of e-learning in Law subjects?*

Four participants have a positive attitude towards the use of digital technologies in Law subjects. They believe that e-learning tools are extremely useful and suitable for some teaching activities. One participant (P3) pointed out that traditional teaching methods are no longer suitable for today's students and that the interaction and engagement of students in classes can be improved with the use of digital technologies and an online learning environment:

„I think that it can be very useful. It can lead to the transformation of the learning methods, which are not so adequate for today's students. The traditional way of lecturing, especially at Law schools where we're having 3 to 4 hours of only lectures in the classroom can't be successful in the means of having the attention of the students for the whole time. The lectures need to be interactive and with the participation of the students. I think that online environment can contribute to that."

Two participants (P3, P4) are still reluctant regarding the use of e-learning in Law courses. They find that e-learning is not applicable in all fields of Law and all domains of higher education.

2. *Have you yourself attended any MOOC? If yes, how did you find it? If not, why not?*

Half of the participants(n=3) did not have any experience with MOOCs as they did not find time to attend them. Another half of the participants have enrolled on some MOOCs, some of them (P3, P4) just because of the project to get an idea of what a MOOC should look like. Only one participant actively participated in some MOOCs and he/she liked the flexibility of such courses.

3. *What is your attitude towards developing MOOC in the DIGinLaw project? How did you perceive this task (easy, difficult, unrealistic,..)?*

Three participants had some big concerns before starting MOOC development as they did not have enough knowledge and experience about it and they knew that the process would be rather complex and demanding. The process of MOOC development itself had shown them to be reachable in the end. They learned a lot and they reconsidered their teaching methods. In the end, they enjoyed the whole process.

One of the participants (P4) pointed out that in online teaching and learning, he/she misses the social element through which teachers get feedback about his/her teaching.

„It was a challenge. It made me think about teaching in different way. It made me think more about the outcome – what I wanted the students to learn and to think about this much more than I do in general. When I teach in class I heavily rely on the reactions of the students - looking at their faces and change or come back to an idea if I have the feeling that they are not understanding or giving an example or moving faster if I realised that they are confident with the subject."

The other three participants have a positive opinion about MOOC development and found some processes quite realistic. During MOOC development, they found that some steps in the MOOC development are harder than they thought,

and some are easier, but in the end reachable. They have also pointed out that it was all new for them, and that they have a positive view of the process.

Adaptability

1. *How did you prepare for the development of the MOOC?*

All participants find that the organized training they had before the MOOC development was a good starting point. Five participants first developed all learning material, and then with the support of their colleagues and SRCE and the available online course "Digital competences of HE teachers for innovative teaching practices" started to develop the MOOCs. After that, they worked on MOOC improvement to make it self-paced. Only one participant (P2) tried to visualise and develop a structure of his/hers MOOC before putting learning material into the course and adapting it to be self-paced. After developing the course structure, the next step was putting learning materials into an online environment.

2. *Was your previous experience in teaching and use of digital technologies enough to start with the preparation and development of MOOCs?*

Four participants stated that their previous experience with teaching and the use of digital technologies was not enough to prepare and develop MOOCs. Two participants (P1, P2) find their previous experience in combination with training about basics in Moodle (organized by the SRCE team) was enough for the preparation and development of MOOCs.

3. *How much did you rely on support in the preparation of MOOC? What kind of support did you need? Technical, learning design, video preparation, pedagogical,…?*

All participants stated that they need some kind of support in MOOC development, some needed technical support in the use of Moodle and some pedagogical support in defining teaching methods. Some have relied on the support of their colleagues. All participants have prepared learning materials on their own.

4. *How did you prepare learning materials for MOOC? used existing ones, prepared new ones?*

All participants have developed new materials for MOOCs, and one (P2) has used some existing learning materials available in free access (open educational resources).

Advantages and disadvantages

1. *Based on your experience in the use of digital technologies and e-learning so far, can you identify some advantages and disadvantages?*

Participants recognize that digital technologies and e-learning can bring advantages to education, such as flexibility in the learning process; students have grown up with new technologies and use them very well; better student engagement in the teaching and learning process; learning materials are constantly available to students. One participant (P1) also focused on the advantages that digital technologies bring to teachers: the teacher can teach from a remote location, student evaluation is much faster and more effective; the system is more precise, and the discussion in class is better.

Teachers singled out as the main disadvantage of digital technologies and the e-learning time required to learn how to work with them, the lack of social aspects in online classes (students disconnect and do not participate), lack of social contact and difficulty to assess students' knowledge online.

2. *Now that you have developed MOOC, what advantages/disadvantages do you see in such a way of teaching? Would you copy this experience and way of teaching and learning to other courses?*

The teachers participating in the survey see as advantages of MOOCs that students can better organize their own learning, that they are given more autonomy; learning takes place all the time (not subject to other influences) and is accessible to everyone. Some disadvantages that the participants mentioned were hacker attacks, and lack of social contact.

Most of the participants would use this type of teaching in their own e-courses. One participant (P1) pointed out that he/she likes this way of teaching because it is more efficient for the teacher in the long term, and the students are provided with a better quality of education:

„Yes, of course, I would. This way of teaching requires you to prepare much more, so in the preparation phase you have to devote much more time and energy but then once you have that all set up, the actual teaching is much easier and you have to put in a lot less energy than in classical teaching. In a long term, this is easier for teachers and I think students get more quality."

3. *Do you find your digital skills enough for the preparation of MOOCs and e-courses? Do you think that teachers' professional development in digital skills should be compulsory?*

Three participants found their digital skills sufficient for the development of MOOC and e-courses, and they improved them working on this project. Two participants (P1, P2) stated that they attended some courses that helped them when creating MOOCs, but also that the key to everything is the constant use of technology because the acquired knowledge is forgotten if not used. Most of the participants (n=5) believe that professional development in digital skills must be mandatory.

4. *How important is support to teachers in the use of e-learning and new teaching methods? How should it be organized?*

All participants find that support for teachers in using of e-learning and new teaching methods is essential. They pointed out that universities and faculties must provide such support to teachers in the form of workshops, courses and consultations. One participant (P3) also emphasized the importance of personal motivation in the whole process:

„*Of course, they should not be alone, particularly those that are inexperienced. Teachers must be motivated and they must have some initial training but after that, they have to try on their own. Because the content you want to create is something that you have in mind and you know why certain sentence or idea or knowledge is important and you know how to make it compulsory for student or interesting; so it's something that can't be taught or supported. You need support from the beginning and you need constant support about methodologies, but you have to try. So it's a process that really is dependent on the motivation of each teacher."*

5. *Would you recommend the use of e-learning and the development of MOOCs to other colleagues?*

All participants would recommend the use of e-learning and the creation of MOOCs to their colleagues. Additionally, one participant (P6) expressed the opinion that hybrid and online classes are the future of education:

„Yes, I would definitely recommend that. I think it's an excellent experience and it really increases our capabilities as teachers in higher education and I think it's good for the students, it's good for us as teachers because I think that's the future of education. I know students still like face-to-face elements but I think that some sort of hybrid learning is probably where the future will be going."

3.3. Discussion and concluding remarks

This paper outlines the example of providing support to teachers in the development of MOOCs. Support to Law teachers in the development of MOOCs was organized within the Erasmus+ project DIGinLaw.

Although without experience in the design of MOOCs and even without knowing how a MOOC should look like, Law teachers participating in the DIGinLaw project were able to design successfully a MOOC with the proper training and support. Training and support in this project were organized in the following way:

- identification of participants (teachers) and setting of the training strategy
- training adapted to participants (tailor-made)
- preparation of the Course Design Form (to help participants recognize all parts of course design)
- preparation of a Template on MOOC design
- providing continuous support to participants in course development (consultations one on one, and consultations for a group of participants) on technical issues and on learning design
- evaluation of the designed courses with recommendations for improvements
- final evaluation of MOOCs.

In order to verify the proposed training programme and get feedback from teachers about their experience with MOOC development, the E-learning Centre team conducted research. As the research method, semi-structured interviews were chosen. The interviews were done with teachers participating in the project who volunteered to participate in the research.

The proposed hypothesis that training and support provided to teachers by the SRCE ELC team was enough for teachers to be able to design their first MOOC has been confirmed in the research.

The second hypothesis has been also verified in the research. Most teachers are more open to the use of digital technologies in teaching and recognize the benefits digital technologies can bring to the educational process.

The research results showed the importance of support to teachers in the process of designing and developing MOOCs. No less important is creating a positive environment in which they work so that they are motivated to foster excellence in teaching and use of digital technologies to improve the quality of the educational process. Teachers' digital competences in ICT and e-learning are crucial to enable them to choose the right digital technologies for purpose of their teaching and know how to integrate them into the educational process. User support is one of the important factors in process of the implementation of ICT and e-learning technologies into the educational process. Knowledge of working with ICT and e-learning technologies is not enough. Lack of support and training in new pedagogical methods and technologies can particularly affect teachers who do not feel

comfortable with them.[25] [26] [27] It is, therefore, necessary to provide teachers with training to gain knowledge on how to improve their pedagogical practice, how to replace traditional teaching and incorporate new educational models that place students at the centre of the educational process.[28] An important factor is an available infrastructure in terms of the availability of e-learning tools and technologies, IT support and stable internet connection According to this, it can be concluded that the skills and competencies of teachers, especially competencies related to ICT and pedagogical competencies, are necessary for the adoption of e-learning.[29] Results from research titled Higher education teachers and pandemic: academic and psychological challenges done in 2021 by the Agency for Higher Education and Science [30] on a sample of 1204 teachers show that support is very important in preparation and conducting online teaching and learning. Support in the preparation and development of e-courses is considered extremely important and important to 78% of teachers, and 76% of teachers need support related to pedagogy and teaching methods. Comparing these results to those of the present research, we can see a correlation. Institutions that have successfully deployed new learning technologies provided technical support and training for students and guidance for faculty on how to adapt their course content and delivery.[31]

Experience gained during the pandemic certainly influenced teachers' readiness to use digital technologies and to develop MOOCs. Although finding the design of MOOC challenging at the beginning, most of the participants, in the end, were satisfied with the results, knowledge and experience they gained.

The SRCE ELC has a long time of experience in supporting teachers in the design and development of e-courses and providing training for teachers, nevertheless, this was a new and exciting experience for them as well. Working with teachers

---

25 Kučina Softić, S., *Teachers' digital competences as a key factor for the digital transformation of education*, *Advances in Online Education: A Peer-Reviewed Journal*, Vol. 1, No. 1, 2022, pp. 75-86.

26 Buabeng-Andoh, C., *Factors influencing teacher's adoption and integration of information and communication technology into teaching: a review of the literature,* IJEDICT, Vol. 8, No. 1, 2021, pp. 136-155.

27 Mahdizadeh, M.; Biemans, H.; Mulder, M., *Determining factors of the use of e-learning environments by university teachers*, Computers& Education, Vol. 51, No. 1, 2008, pp. 142-154.

28 Bennett, S.; Lockyer, L.; Agostinho, S., *Towards sustainable technology-enhanced innovation in higher education: Advancing learning design by understanding and supporting teacher design practice,* British Journal of Educational Technology; Vol. 49, No. 6, 2018, pp. 1014-1026.

29 Jokiaho, A.; May, B.; Specht, M. S. S., *Barriers to using E-learning in an Advanced Way,* International Journal of Advanced Corporate Learning, Vol. 11, No. 1, 2018, pp. 17-22.

30 Agencija za znanost i visoko obrazovanje, Sveučilišni računski centar Sveučilišta u Zagrebu, Sveučilište u Rijeci, *Visokoškolski nastavnici i pandemija: akademski i pshiološki izazovi*, Zagreb, 2021.

31 Brasca, C., Marya, V., Charag, K., Owen K., Sirois, J., Ziade, D., *How technology is shaping learning in higher education,* McKinsey&Company, 2022, [https://www.mckinsey.com/industries/education/our-insights/how-technology-is-shaping-learning-in-higher-education], Accessed 20 February 2023.

from different universities and from different countries provided new and important insight into the needs of teachers when using digital technologies to adapt education to the digital age.

The presented model of teachers' training and support in the use of digital technologies to develop MOOCs can be adapted to similar situations. The online course "Digital competences of HE teachers for innovative teaching practices" (https://mod.srce.hr/course/view.php?id=391) is open to everyone and is open access and can be used for further training of teachers in digital technologies.

REFERENCES

BOOKS AND ARTICLES

1. Bates, A.W., *Teaching in a Digital Age,* Third Edition, Tony Bates Associates Ltd., Vancouver, B.C., 2021
2. Bond, M.; Bedenlier, S.; Marín, V.I. *et al., Emergency remote teaching in higher education: mapping the first global online semester,* Int J Educ Technol High Educ, Vol. 18, 50, 2021, pp. 1-24
3. Bennett, S.; Lockyer, L.; Agostinho, S., *Towards sustainable technology-enhanced innovation in higher education: Advancing learning design by understanding and supporting teacher design practice*, British Journal of Educational Technology, Vol. 49, No. 6, 2018, pp. 1014-1026
4. Brown, M., *What are the Main Trends in Online Learning? A Helicopter View of Possible Futures,* Asian Journal of Distance Education, Vol. 16, No. 2, 2022, pp. 118-143
5. Buabeng-Andoh, C., *Factors influencing teacher's adoption and integration of information and communication technology into teaching: a review of the literature*, IJEDICT, Vol. 8, No. 1, 2021, pp. 136-155
6. Creswell, J. W., *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.), Sage, 2011
7. Gaebel, M.; Zhang, T.; Stoeber, H. &. M. A., *Digitally enhanced learning and teaching in European higher education institutions,* European University Association, Brussels, 2021
8. Jokiaho, A.; May, B.; Specht, M. S. S., *Barriers to using E-learning in an Advanced Way*, International Journal of Advanced Corporate Learning, Vol. 11, No. 1, 2018, pp. 17-22
9. Kavarić M.; Kavarić A.; Djokovic R., *Challenges in online teaching during COVID-19 pandemic: Higher education survey in Montenegro*, Innovations in Education and Teaching International, 2021
10. Kučina Softić, S., *Digitalne kompetencije nastavnika za primjenu e-učenja u visokom obrazovanju*, Zagreb, 2020, doctoral thesis
11. Kučina Softić, S.; Lasić Lazić, J.; Tropša, V., *Analiza ankete o stavu nastavnika prema tehnologijama e-učenja u visokom obrazovanju te koje digitalne kompetencije su im potrebne kako bi na kvalitetan način primijenili e-učenje u obrazovnom procesu*, Sveučilište Sjever, Koprivnica, 2022

12. Kučina Softić, S.; Odak, M.; Lasić Lazić, J., *Digitalna transformacija: Novi pristupi i izazovi u obrazovanju*, Sveučilište Sjever, Koprivnica, 2021
13. Kučina Softić, S.; Radobolja, T; Martinović, Z., *How did we support education in pandemic-role of the e-learning centre*, EDEN Digital Learning Europe Proceedings, 2022 Annual Conference Tallinn, 20-22 June 2022, pp. 37-42
14. Kučina Softić, S., *Teachers' digital competences as a key factor for the digital transformation of education*, Advances in Online Education: A Peer-Reviewed Journal, Vol. 1, No. 1, 2022, pp. 75-86
15. Kumi-Yeboah, A.; Sallar, A.W.; Kiramba, L.K.; Kim. Y., *Exploring the use of digital technologies from the perspective of diverse learners in online learning environments,* Online Learning, Vol. 24, No. 4, 2020, pp. 42-63
16. Mahdizadeh, M.; Biemans, H.; Mulder, M. *Determining factors of the use of e-learning environments by university teachers*, Computers& Education, Vol. 51, No. 1, 2008, pp. 142-154
17. Merriam, S. B., *Qualitative Research: A Guide to Design and Implementation,* Jossey-Bass, 2009
18. Zhang, T., *National Developments in Learning and Teaching in Europe*, European University Association, Brussels, 2022
19. Župan, M., *Online Legal Education in Croatia*, in: Nottage, L.; Ibusuki, M. (eds.), Comparing Online Legal Education, Intersentia, Cambridge, 2022

REPORTS

1. Agencija za znanost i visoko obrazovanje, Sveučilišni računski centar Sveučilišta u Zagrebu, Sveučilište u Rijeci, *Visokoškolski nastavnici i pandemija: akademski i pshiološki izazovi*, Zagreb, 2021
2. Brooks, D.C.; McCormac, M., *EDUCAUSE: Driving Digital Transformation in Higher Education*, ECAR research report, ECAR, Luisville, 2020
3. Brown, M.; Connole, G.; Beblavy, M., *Education outcomes enhanced by the use of digital technology: Reimagining the school learning ecology*, EENEE Analytical Report No. 38, Luxemburg, 2019

WEBSITE REFERENCES

1. Brasca, C.; Marya, V.; Charag, K.; Owen K.; Sirois, J.; Ziade, D., *How technology is shaping learning in higher education,* McKinsey&Company, 2022, [https://www.mckinsey.com/industries/education/our-insights/how-technology-is-shaping-learning-in-higher-education], Accessed 20 February 2023
2. DIGinLaw project web page, [https://www.pravos.unios.hr/diginlaw/], Accessed 8 February 2023
3. E-learning Centre at the University Computing Centre, University of Zagreb, [https://www.srce.hr/elc], Accessed 8 February 2023
4. European Commission, *Digital Education Action Plan 2021-2027: Resetting Education for Digital Age*, Brussels, 2020, [https://education.ec.europa.eu/focus-topics/digital-education/action-plan], Accessed 10 December 2022

5. European Commission, *European Education and Training Expert Panel: Summary of findings and of the discussions at the 2019 Forum on the Future of Learning*, Luxemburg, 2019, [https://op.europa.eu/en/publication-detail/-/publication/b976dfa7-a6a9-11e9-9d01-01aa75ed71a1/language-en], Accessed 10 December 2022
6. European Commission, *European Universities Initiative Survey on the impact of COVID-19 on European Universities,* 2020, [https://erasmus-plus.ec.europa.eu/document/coronavirus-european-universities-initiative-impact-survey-results], Accessed 10 February 2023
7. University Computing Centre, University of Zagreb, [https://www.srce.hr], Accessed 8 February 2023
8. WEF, *The future of jobs*, 2020, [https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf], Accessed 10 February 2023

ISBN 978-953-8109-56-0