COLLANA L'UNITÀ DEL DIRITTO 53

LAW AND SOCIAL CHANGE

a cura di BEATRICE BICHI RUSPOLI FORTEGUERRI, FEDERICO BONITO

RomaTrE-Press
2025

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Nella stessa Collana

1. P. Carnevale (a cura di), *La Costituzione riscritta. Saggi sulla revisione costituzionale in itinere*, 2016
2. E. Battelli, B. Cortese, A. Gemma, A. Massaro (a cura di), *Patrimonio culturale: profili giuridici e tecniche di tutela*, 2017
3. R. Benigni (a cura di), *Libertà religiosa, diritti umani e globalizzazione*, 2017
4. A. Massaro (a cura di), *La tutela della salute nei luoghi di detenzione. Un'indagine di diritto penale intorno a carcere, REMS e CPR*, 2017, 2017
5. V. Zeno-Zencovich, *Comparative Legal Systems. A Short Introduction*, 2017 (I ed.) *Comparative Legal Systems. A Short and Illustrated Introduction*, 2019 (II ed.)
6. M. Gambacciani, *Impresa e lavoro: il nuovo bilanciamento nei licenziamenti collettivi*, 2017
7. A. Massaro, M. Sinisi (a cura di), *Trasparenza nella P.A. e norme anticorruzione: dalla prevenzione alla repressione*, 2017
8. A. D. De Santis (a cura di), *I profili processuali della nuova disciplina sulla responsabilità sanitaria*, 2017
9. V. Viti, *La locazione finanziaria tra tipicità legale e sottotipi*, 2018
10. C. Cardia, R. Benigni (a cura di), *50 Anni dalla Populorum Progressio. Paolo VI: il Papa della modernità. Giustizia tra i popoli e l'amore per l'Italia*, 2018
11. G. Nuzzo, *L'abuso del diritto di voto nel concordato preventivo. Interessi protetti e regola di correttezza*, 2018
12. G. Grisi, C. Salvi (a cura di), *A proposito del diritto post-moderno. Atti del Seminario di Leonessa, 22-23 settembre 2017*, 2018
13. G. Maestri, *L'ordinamento costituzionale italiano alla prova della democrazia paritaria*, 2018
14. G. Conte, A. Fusaro, A. Somma, V. Zeno-Zencovich (a cura di), *Dialoghi con Guido Alpa. Un volume offerto in occasione del suo LXXI compleanno,* 2018
15. E. Poddighe, *Comunicazione e "dignità della donna". Uno studio di genere*, 2018
16. G. Grisi (a cura di), *L'abuso del diritto. In ricordo di Davide Messinetti*, 2019
17. S. Anastasia, P. Gonnella (a cura di), *I paradossi del diritto. Saggi in omaggio a Eligio Resta*, 2019
18. S. Del Gatto, *Poteri pubblici, iniziativa economica e imprese*, 2019
19. R. Benigni, B. Cortese (a cura di), *La "giurisdizione". Una riflessione storico-giuridica*, 2019

20. M. Ruotolo (a cura di), *La Costituzione...aperta a tutti*, 2019 (I ed.); M. Ruotolo, M. Caredda (a cura di), *La Costituzione...aperta a tutti*, 2020 (II ed.); M. Ruotolo, M. Caredda (a cura di), La Costituzione...aperta a tutti, 2021 (III ed.); M. Ruotolo, M. Caredda (a cura di), La Costituzione...aperta a tutti, 2022 (IV ed.)
21. N. Posteraro, M. Sinisi (a cura di), *Questioni di fine vita,* 2020
22. G. Resta (a cura di), *L'Armonia nel diritto. Contributi a una riflessione su diritto e musica,* 2020
23. F. Lattanzi (a cura di), *Genocidio. Conoscere e ricordare per prevenire*, 2020
24. E. Toti, *Diritto cinese dei contratti e sistema giuridico romanistico tra legge e dottrina*, 2020
25. B. Cortese, *La tutela in caso di vizio della* res empta *e della* res locata*: inadempimento rispondenza* ex fide bona, 2020
26. M.S. Bonomi, *La motivazione dell'atto amministrativo: dalla disciplina generale alle regole speciali,* 2020
27. G. Grisi, F. Rassu (a cura di), *Perspectives nouvelles du droit. Thèmes, méthodes et historiographie en France et en Italie,* 2020
28. F. Aperio Bella, A. Carbone, E. Zampetti (a cura di), *Dialoghi di Diritto Amministrativo. Lavori del Laboratorio di Diritto Amministrativo 2019*, 2020
29. S Caldarelli, *I vincoli al bilancio dello Stato e delle pubbliche amministrazioni. Sovranità, autonomia e giurisdizione*, 2020
30. A. Massaro (a cura di), *Connessioni di Diritto Penale*, 2020
31. R. Benigni (a cura di), *Diritto e religione in Italia*, 2021
32. E. Calzolaio, R. Torino, L. Vagni (a cura di), Liber amicorum *Luigi Moccia*, 2021
33. A. Carratta (a cura di), *Limiti esterni di giurisdizione e diritto europeo. A proposito di Cass. Sez. Un. n. 19598/2020*, 2021
34. M. Catenacci, R. Rampioni, V.N. D'Ascola (a cura di), *Studi in onore di Antonio Fiorella*, 2021
35. F. Grassi, O. Hagi Kassim (a cura di), *Vecchie e nuove certezze nel diritto amministrativo. Elementi essenziali e metodo gradualista. Dibattito sugli scritti di Giampaolo Rossi*, 2021
36. B. Cortese (a cura di), *Il diritto dei beni culturali. Atti del Convegno OGIPAC in memoria di Paolo Giorgio Ferri. Roma 27 maggio 2021*, 2021
37. V. Mannino, *Governo misto romano e repubblicanesimo americano*, 2022
38. V. Bontempi (a cura di), *Lo Stato digitale nel piano di ripresa e resilienza,* 2022
39. E. Battelli, M. Lottini, G. Spoto, E.M. Incutti, (a cura di), *Nuovi orizzonti sulla tutela degli animali*, 2022
40. F. Aperio Bella, A. Carbone, E. Zampetti (a cura di), *Dialoghi di diritto amministrativo. Lavori del laboratorio di diritto Amministrativo 2020-2021*, 2022

41. J.M. Peris Riera, A. Massaro, *Derecho Penal, Inteligencia Artificial y Neurociencias. Diritto Penale, Intelligenza Artificiale e Neuroscienze*, 2023
42. A.D. De Santis, *La disapplicazione dell'atto amministrativo nel processo civile. Premesse per uno studio*, 2023
43. F. Ruggeri, *Poteri privati e mercati digitali. Modalità di esercizio e strumenti di controllo*, 2023
44. E. Rigo (a cura di), *Per una ragione artificiale. In dialogo con Lorenzo d'Avack su Costituzione, ordine giuridico e biodiritto*, 2023
45. C. Salvi, *Cinquant'anni di scritti giuridici*, 2024
46. D. Chinni, L. Pace (a cura di), *Il Referendum abrogativo dopo la tornata del 2022. Nuove tendenze e nodi irrisolti*, 2024
47. V. Zeno-Zencovich, *Il futuro dell'Accademia. Scritti dedicati agli allievi*, 2024
48. F. Aperio Bella, A. Carbone, E. Zampetti (a cura di), *Dialoghi di diritto amministrativo. Lavori del laboratorio di diritto Amministrativo 2022-2023*, 2024
49. F. Rimoli, S. Talini, *"Si vis pacem, para bellum"? La guerra e le democrazie europee. Atti del convegno annuale dell'OSDE, Roma 16 febbraio 2024*, 2024
50. G. Fiorelli, E. Fronza, N. Guzmán, D. Ippolito, L. Marafioti (a cura di), *Verità e giustizia nel processo penale. Atti del convegno di studi giuridici organizzato dalle Università di Bologna, Buenos Aires e Roma Tre (18-22 gennaio 2024)*, 2025
51. S. Benvenuti, G. Rossetti (a cura di), *La Garanzia. Tradizioni storiche e modelli*, 2025
52. F. Borlizzi, S. Zolea (a cura di), *Cliniche legali, culture giuridiche e trasformazioni sociali. Un dialogo italo-cubano*, 2025

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

COLLANA L'UNITÀ DEL DIRITTO 53

LAW AND SOCIAL CHANGE

2024 International Doctoral Workshop

a cura di
BEATRICE BICHI RUSPOLI FORTEGUERRI, FEDERICO BONITO

RomaTrE-Press
2025

La Collana *L'unità del diritto* è stata varata su iniziativa dei docenti del Dipartimento di Giurisprudenza. Con questa Collana si intende condividere e sostenere scientificamente il progetto editoriale di Roma Tr*E-Press*, che si propone di promuovere la cultura giuridica incentivando la ricerca e diffondendo la conoscenza mediante l'uso del formato digitale ad accesso aperto.

Collana pubblicata nel rispetto del Codice etico adottato dal Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, in data 22 aprile 2020.

Il volume pubblicato è stato sottoposto a previa e positiva valutazione nella modalità di referaggio *double-blind peer review.*

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Caratteri tipografici utilizzati:
Day Roman, Iowan Old Style (copertina e frontespizio)
Adobe Garamond Pro (testo)

Impaginazione e cura editoriale: Colitti-Roma colitti.it

Edizioni: Roma TrE-Press
Roma, dicembre 2025
ISBN: 979-12-5977-527-6
http://romatrepress.uniroma3.it

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Collana del Dipartimento di Giurisprudenza

L'unità del diritto

La Collana di studi giuridici promossa dal Dipartimento di Giurisprudenza dell'Università Roma Tre assume un titolo – quello de *L'unità del diritto* – che può apparire particolarmente impegnativo, perché il fenomeno giuridico riflette la complessità delle società che il diritto mira a regolare, si sviluppa intorno ad una molteplicità di articolazioni e sembra pertanto sfuggire ad una definizione in termini di unità. Anche la scienza del diritto, intesa come riflessione intorno al diritto, come forma di conoscenza che assume il diritto ad oggetto diretto e immediato di indagine, sia nella prospettiva teorica sia in quella storico-positiva relativa ad un singolo ordinamento, soffre a trovare una sua dimensione unitaria. La riflessione intorno al diritto, da qualunque punto di partenza si intenda affrontarla, ammette una pluralità di opzioni metodologiche, contempla una molteplicità di giudizi di valore, si caratterizza inevitabilmente per una pluralità di soluzioni interpretative. L'unico, generalissimo, elemento che sembra contraddistinguerla in senso unitario è dato dal suo essere rivolta alla conoscenza del diritto, dal suo carattere conoscitivo dell'esperienza giuridica complessivamente intesa, una unità, potrebbe dirsi, figlia della diversità e varietà delle scelte di metodo e del pluralismo interpretativo, ma pur sempre una unità quanto meno in questo suo nucleo irriducibile. Ed è allora questo il senso da attribuire al titolo della collana che prende l'avvio, ossia quello di dare ospitalità a contributi di studiosi diversi per formazione e interessi, ma che si riconoscono tutti nella comune esigenza di indagare il fenomeno giuridico applicando con rigore il metodo prescelto, nella consapevolezza della condivisione di un patrimonio formativo e culturale idoneo a creare un'adeguata coscienza di sé e sulla cui base costruire l'impegno scientifico del giurista.

In questa prospettiva, la Collana si ripromette di ospitare non solo contributi scientifici di tipo monografico, raccolte di scritti collettanee, atti di convegni e seminari, ma anche materiali didattici che possano proficuamente essere utilizzati nella formazione dei giovani giuristi.

La Collana entra a far parte della struttura di Roma Tr*E-Press*, che, affiancando alla tradizionale pubblicazione in formato cartaceo quella in formato digitale in *open access*, contribuisce ad una nuova e più ampia diffusione del sapere giuridico.

Prof. Antonio Carratta
Direttore del Dipartimento di Giurisprudenza
Università Roma Tre

Table of Content

Giorgio Pino*

Foreword

The university is one of the places – not the only one, but probably the most prominent indeed – to which our societies assign the role of producing new knowledge, and of transmitting it to students, as well as to society as a whole. In the pervasive economic and bureaucratic-corporate language that follows almost every aspect of our lives, these different but closely intertwined dimensions of university life have even been labelled as the three 'missions' of the university – that is, 'tasks' to be carried out, and obviously reported on – according to a mindset that seems to reject the notion that society can enormously benefit, in various ways, even from 'pure' research activities, researches that are ends in themselves and are not linked to immediate concrete applications.

Now, over the course of a researcher's life a PhD (or doctoral program) is still one of the few places or stages where it is possible to choose a research topic, and explore it for three to four years, simply because that topic is 'interesting'. The only thing that is asked, and that should be asked, of doctoral students is to identify a topic that is worth spending their intellectual energy on, and to devote themselves to it with energy and enthusiasm, and with the healthy ambition to say something new about that topic. More generally, the years spent in a doctoral program are undoubtedly the most formative period in the life of a scholar: the readings and discussions that happen during those years are often decisive – in one way or another – for the rest of a scholar's intellectual life.

This takes us to ask how a doctoral program – understood as an organizational structure within a university department – can create the best conditions for young scholars to develop their potential, in a way that will positively shape the rest of their intellectual life. Certainly, one condition is that each doctoral student finds a valid scientific mentor who believes in in his research, and in his capacity to develop it, and who encourages him above all in pursuing critical and independent thinking. Another condition is that, during their doctoral studies, students are

* Professor of Philosophy of Law, Università Roma Tre. Director, Doctoral Program in Law & Social Change.

exposed to a variety of ideas and approaches, which do not necessarily have to be closely related to the doctoral student's research topic. On the contrary, it is preferable that the several cultural activities organized by the doctoral program are relatively diverse and expose students to topics and methodologies that they would probably not have encountered on their own. Finally, another condition, and no less important, is that doctoral students find themselves in a collegial environment that encourages discussion among peers on their ongoing doctoral research: this is because research can, in principle, be a rather solitary activity, with long hours spent on studying and writing, and often the simple act of explaining the content and potential significance of one's research to other doctoral students brings to light hidden corners, unexpected problems, and the need for clarifications that one had not considered before.

This last consideration was precisely the drive that led, as early as 2023, a group of PhD students from the Law & Social Change program at Roma Tre University to launch the idea of an International Doctoral Workshop, in which numerous PhD students from various European universities could meet and discuss their ongoing research – first and foremost with other doctoral students. This workshop is entirely managed by doctoral students – from securing the necessary funds to selecting the papers to be presented in Rome, to editing the volume that you are now reading. I cannot congratulate enough with our doctoral students the workshop, an especially with the editors of the present volume, Beatrice Bichi Ruspoli Forteguerri and Federico Bonito, for all their splendid work.

This volume contains a selection of the papers presented at the 2024 edition of our International Doctoral Workshop, and the topics chosen by the speakers are already highly revealing of the scientific interests that drive the new generations of scholars: the impact of new technologies on various aspects of law (public administration, criminal procedural law, media regulation), and environmental protection are now unavoidable issues on which the new generation of scholars will inevitably be called upon to make their mark.

These types of topics, moreover, are precisely what inspired the launch of the Law & Social Change doctoral program in the first place: since its inception, this doctoral program has been designed to encourage innovative research that looks at law and legal culture – as well as the processes of law production and application – with cross-cutting perspectives with respect to national and supranational dimensions, public and private dimensions, substantive and procedural dimensions, formal and informal dimensions. The doctoral program in Law & Social Change is open to any disciplinary

field and encourages research paths that are innovative in nature and interdisciplinary and multidisciplinary in nature.

For all these reasons, I am extremely proud, as the Director of the Law & Social Change doctoral program, to now witness the publication of this volume, which brings together the contributions presented at the 2024 edition of our International Doctoral Workshop, and with the hope that more workshops, and volumes, of this kind will come in the future.

Beatrice Bichi Ruspoli Forteguerri[*], Federico Bonito[**]

Introductory Remarks

The PhD program in Law & Social Change at Roma Tre University has been honored to sponsor the initiative of the International Doctoral Workshops, launched in 2023 and conceived by its doctoral candidates. This volume gathers the contributions presented during the 2024 edition of the Workshop, offering readers a glimpse into the debates and research trajectories of young legal scholars. As members of the organizing committee of this edition, we wish to briefly recall the vision that inspired the series and the role it has played within our doctoral community.

The idea underlying the International Doctoral Workshop series does not come from afar. As PhD candidates enrolled in an international doctoral curriculum, we have consistently recognized the necessity for a forum dedicated to the exchange of ideas, the interrogation of methodologies, and the testing of preliminary findings, a forum that extends beyond the confines of a single academic institution. Our aim was to create a collegial environment, fostering rigorous and engaging intellectual discourse among peers. It was this vision that led us, as colleagues at Roma Tre University, to devise a series of International Doctoral Workshops where emerging academics could debate their research, offer constructive criticism of one another's work, and, ultimately, find a receptive audience among their peers.

This vision was first realized with the inaugural International Doctoral Workshop in 2023. From the outset, the initiative was guided by three main principles. First, thematic breadth. The event focused on contemporary phenomena that challenge traditional legal concepts and dichotomies - such as national/international, public/private, substantive/procedural - while deliberately embracing a broad range of perspectives and approaches. Second, in-person exchange. Presentations and discussions were held face-to-face, with more than twenty PhD candidates and postdocs attending from Europe and beyond. Beyond the immediate intellectual benefits, the workshop succeeded in forging a strong network of junior scholars across

[*–**] PhD student at Roma Tre University.

a wide range of European and global institutions. Third, the central role of junior scholars. Participation was deliberately limited to PhD candidates and early-career researchers, in order to preserve a truly horizontal and welcoming atmosphere. Professors and senior researchers from Roma Tre University supported the initiative as discussants, offering guidance while leaving the intellectual stage primarily to junior participants.[1] The outcome exceeded our own expectations, leaving us impressed by the level of engagement and debate. The presentations were truly stimulating, as we exchanged ideas and confronted our legal traditions.

Encouraged by the success of the inaugural edition, we set out to organize a new edition in 2024. Following the core features and lessons learned in the previous year, the workshop once again provided an open forum for doctoral candidates and postdoctoral fellows to present innovative research on modern legal challenges. However, we introduced a key ambition for the 2024 edition: to create a tangible and lasting contribution to the scholarly community by publishing the presented research. The objective was twofold: to disseminate the excellent work of our participants and to offer a supportive, peer-driven avenue for publication. We believed this to be a critical step for career progression within today's academia, often marked by a "publish-or-perish" culture.[2]

This collected volume represents the culmination of that ambition. Following the workshop, we partnered with Roma TrE-Press, whose guidance was instrumental in bringing the project to fruition. In order to achieve this, the intercession and support of Professor Vincenzo Zeno-Zencovich and Professor Giorgio Pino were invaluable. To ensure scholarly rigor, we implemented a cross-blind peer-review process, wherein each contributing author anonymously reviewed a fellow participant's paper. The result of this collaborative and meticulous process is the volume you now hold.

The book is divided into self-contained chapters tackling different issues concerning the law, such as the relationship between law and different modern concepts, including technology, mass media, climate and sustainability, and cultural and philosophical traditions.

In chapter I, Igor Gontarz assesses the impact of the AI Act on the

[1] In this regard, we would like to thank Professors Giuseppe Palmisano, Simone Benvenuti, Giorgio Pino and Fiona MacMillan, as well as Doctors Morgan Harris and Alba Lojo.

[2] The literature on "publish or perish" is astonishingly vast. See, generally, P.F. Postelwaite, *Publish or Perish: The Paradox*, in *Journal of Legal Education*, 2000, vol. 500, 20, 157 – 188.

automation of public administration, questioning whether it constitutes a true paradigm shift. The paper argues that the Act introduces game-changing requirements for transparency and accountability for high-risk AI systems, yet its narrow definition of AI leaves many automated decision-making tools unregulated, creating a need for complementary national legislation.

In chapter II, Afroditi Papathanasopoulou investigates the duty of social media companies under the Digital Services Act to mitigate the negative externalities of disinformation while upholding freedom of expression. The analysis suggests that the DSA's co-regulatory model provides crucial procedural safeguards, but its ultimate effectiveness depends on consistent enforcement and accessible judicial remedies to prevent over-censorship and protect user rights.

In chapter III, Anastasia Nefeli Vidaki explores the potential integration of blockchain technology within the EU criminal justice system, weighing its benefits for transparency and integrity against the significant risks it poses to fundamental rights. The paper concludes that while blockchain presents a major opportunity, a comprehensive legal and ethical framework must be established to address serious concerns about data protection and fairness before any widespread adoption.

In the following chapter, Andreas Kanakakis examines the use of digital investigative measures, such as hacking and AI, in criminal proceedings, framing them as a "double-edged sword". The paper concludes that these powerful tools pose a formidable threat to fundamental rights, particularly privacy and a fair trial, and argues that without clear legal reforms, the balance of power will tilt dangerously in favor of law enforcement.

In chapter V, Ophélie Sémiramis Medza-Mba examines the dangers of media monopolization in France, contextualized by a recent (and since suspended) proposal for audiovisual reform. The paper argues that both State and private media concentration threaten pluralism and democracy. It advocates for a balanced regulatory approach that preserves media independence from both political control and market pressures, ensuring its role as a "fourth estate".

In the following chapter, Federico Di Silvestre analyzes the nature of states' climate finance obligations under international law to assess potential liabilities for non-compliance. The paper argues that a binding collective legal obligation for developed countries exists, supported by the duty to cooperate in international climate law. He concludes, however, that its practical enforcement is severely limited by the absence of clear rules for sharing the financial burden among individual states.

In chapter VII, Davide Sili provides a critical analysis of the U.S. default rules on the co-ownership of jointly developed patents, particularly in the context of eco-sustainability. The paper concludes that the American system, which permits unilateral non-exclusive licensing without a duty to account, risks a "tragedy of the commons" that discourages collaboration, and suggests that introducing a duty of accountability among co-owners would better promote the creation of green innovations.

In the final chapter, Pierre-Emmanuel Rodriguez investigates German legal dogmatics and its contribution to the "scientificity" of law through an epistemological lens. His paper finds that its systematic nature allows for the verification of judicial decisions and scholarly studies, thus enhancing the rationality of law. However, he concludes that this contribution is contingent upon a responsible application that acknowledges the system's inherent ideological influences to avoid its misuse.

Taken together, the chapters of this volume explore a common thread: the ways in which contemporary legal challenges interact with fundamental principles and require innovative, critical, and ethically informed responses. While each contribution addresses a distinct domain, all share a focus on the tensions between emerging technologies, societal transformations, and established legal frameworks, highlighting both opportunities and risks for the protection of rights, transparency, and accountability.

Beyond their individual insights, the chapters collectively showcase the creativity, rigor, and critical engagement of early-career researchers. They illustrate the value of cross-disciplinary and international perspectives in understanding complex legal phenomena, emphasizing that the development of law cannot be disentangled from societal, technological, and ethical contexts.

We hope that this volume will not only present cutting-edge research but also inspire ongoing dialogue and collaboration among emerging scholars. The workshop and the resulting publication represent a shared endeavor to strengthen a network of young legal researchers and to offer a supportive, peer-driven environment where ideas can be debated, refined, and disseminated. It is our hope that the insights contained in these pages will resonate beyond the academic community, contributing to the broader discussion on how law can respond to the challenges of our times.

Igor Gontarz*

Automated public administration through the lens of the AI Act: game changer or just the sound of the future?

1. *Introduction*

On the 13th of June 2024, the European Parliament and the Council adopted a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).[1] The regulation also applies to public administrations seeking to automate their operations using AI systems. The aim of this article is to determine the impact of the AI Act on the implementation of AI systems into public administration. According to the thesis, the AI Act should be regarded as a game changer in the field of automated administration, complementing the existing solutions under the General Data Protection Regulation.[2] Moreover, it supplements the instance-based and judicial control model, which is ill-suited to verify the decision-making process based on algorithms. On the other hand, it is also

* PhD Igor Gontarz, Department of Administrative and Administrative Judicial Procedure, Adam Mickiewicz University in Poznań, https://orcid.org/0000-0002-6138-1244. This article has been prepared as part of research funded by the National Science Centre, project number 2022/45/N/HS5/04260 ("Control of automated decision-making systems employed in administrative proceedings").

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), hereinafter «AI Act».

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

possible to point to parts of the regulation that require improvement and, in a few cases, adaptation of the national administrative law regulation. In this sense, the AI Act may still be a sound of the future, as it does not comprehensively regulate issues related to the automation of public administration activities. The discussion has been divided into a number of sections, dealing respectively with: the definition of AI systems, the high-risk areas, the key requirements of the regulation from the administration's point of view, the changes that the AI Act introduces to the model of judicial review of administration, and the space that, in terms of public administration, has been left to the national legislator. The analysis was made to answer the following questions: 1) To what extent are automated decision-making systems used by the administration subject to the provisions of the AI Act? 2) What obligations will be imposed on public administrations using high-risk AI systems? and 3) To what extent will the control model adopted in the AI Act affect existing control arrangements for administrative activities?

2. *The notion of «AI system»*

According to Article 3 p. 1 of the AI Act, AI system means «a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments». This is a narrower definition than that originally presented in the Commission's proposal, which was accused of being so general that virtually any computer program met the prerequisites for being considered an AI system.[3]

As it derives from recital 12 of the Regulation, «the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations». In literature, there is already discussion on the constitutive elements a system must have to be

[3] M. Namysłowska et al., *O etycznych, prawnych i społecznych konsekwencjach stosowania systemów sztucznej inteligencji w państwach członkowskich Unii Europejskiej. Uwagi na tle projektu rozporządzenia w sprawie sztucznej inteligencji*, in *Przegląd Sejmowy,* vo1. 79 n. 6, 2023, pp. 72–73, <https://doi.org/10.31268/PS.2023.219>.

considered artificially intelligent.[4]

According to the Commission's guidelines on the definition of the AI system, there are seven elements distinguished: (1) a machine-based system; (2) that is designed to operate with varying levels of autonomy; (3) that may exhibit adaptiveness after deployment; (4) and that, for explicit or implicit objectives; (5) infers, from the input it receives, how to generate outputs (6) such as predictions, content, recommendations, or decisions (7) that can influence physical or virtual environments.[5]

Some doubts might arise while interpreting the third element of the definition in Article 3(1) AI Act, which states the system «may exhibit adaptiveness after deployment». According to D. Spałek and J. Rzymkowski, this requirement limits the scope of the term «AI system» exclusively to systems developed within the machine learning approach to AI.[6]

In the opinion of the researchers, this is a piece of the definition that gives actors ample scope for not complying with the AI Act. They come to the surprising conclusion that if a system is trained at the implementation stage and, with the completion of the implementation, the system ceases to be trained because someone who exercises authority over the system decides to prohibit training, such a system is not an AI system according to the definition enshrined in Article 3(1) of the AI Act. Thus, the prohibitions on certain practices listed in Article 5(1) of the AI Act do not apply to such an AI system. In support of their conclusion, they invoke rules of reasoning *a contrario* based on other language versions: Polish, Czech, German, Croatian, Slovakian and Bulgarian. If a system does not have the ability to learn or be learned after it has been implemented, then it is not an AI system.

On the other hand, as the Commission indicates in the Guidelines «the use of the term "may" in relation to this element of the definition indicates that a system may, but does not necessarily have to, possess adaptiveness

[4] D. Spałek; J. Rzymkowski, *Jak nie stosować AI Act na podstawie definicji systemu sztucznej inteligencji.* in *Prawo Nowych Technologii*, n. 2, 2024, p. 21, <https://doi.org/10.32027/PNT.24.2.4>.

[5] Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Brussels, 6.2.2025, C(2025) 924 final.

[6] D. Spałek; J. Rzymkowski, *Jak nie stosować AI Act na podstawie definicji systemu sztucznej inteligencji.* in *Prawo Nowych Technologii*, n. 2, 2024, p. 21, <https://doi.org/10.32027/PNT.24.2.4>.

or self-learning capabilities after deployment to constitute an AI system. Accordingly, a system's ability to automatically learn, discover new patterns, or identify relationships in the data beyond what it was initially trained on is a facultative and, thus, not a decisive condition for determining whether the system qualifies as an AI system».[7] Despite the paramount importance of this interpretation, the guidelines lack further explanation of the presented understanding of the definition. Looking for some arguments, one could indicate an OECD approach according to which different AI systems vary in their adaptiveness and autonomy after deployment.[8] This reading would be compatible with recital 12 of the AI Act, stating notion of «AI system» should be closely aligned with the work of international organisations working on AI.

In my view, a rather broad understanding of the concept of an AI system should be applied so as to limit the possibility of circumventing the obligations arising from it. Treating post-implementation adaptability as a necessary feature of an AI system would lead to depriving the AI Act of its effectiveness vis-à-vis AI systems that pose a significant risk to fundamental rights, including those used by public administration.

However, even with a narrow definition of the term «AI system», which limits the scope to adaptable machine learning models, there are already solutions in public administration that could be considered AI systems. The latter could be ARBUZ (in Polish «Watermelon»), an AI-based tool employed by the Polish consumer protection agency to enforce unfair terms control.[9] As it is mentioned in the Whitepaper on the procurement and development of the tool, «The ARBUZ system continuously analyses standard contract terms and identifies sections as potentially abusive using verified clauses from the database. As the tool is based on supervised machine learning, the analysed standard contract terms also automatically

[7] Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Brussels, 6.2.2025, C(2025) 924 final, paragraph 23.

[8] «An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment». See: OECD Artificial Intelligence Papers, *Explanatory Memorandum on the updated OECD definition of an AI system,* n. 8, 2024, p. 4.

[9] Office of Competition and Consumer Protection, *White paper, Advancing Consumer Law. Enforcement with Artificial Intelligence. Insights from the Polish Office of Competition and Consumer Protection (UOKiK)*, Warsaw 2024, p. 6.

update the original database».[10] There is, therefore, no doubt that the tool will also adapt its operations after the deployment, meeting the requirement of adaptiveness.

Another problem is the relationship between the AI Act and simple decision-support algorithms. Outside the scope of the regulation could be the systems based on decision trees, such as the Dutch SyRi system,[11] especially if the system would be considered as simpler traditional software based on the rules defined solely by natural persons to automatically execute operations in the meaning of the recital 12 of the AI Act. Even more so, it may be difficult to determine unequivocally whether a system constitutes an AI system if this were to be done, for example, by the addressee of an administrative decision issued by an authority. While the Dutch government officially claims that SyRI is a simple decision tree that looks for anomalies in the data, Van Bekkum and Zuiderveen-Borgesius point out that the legislation under which SyRI operates also allows for other algorithmic techniques. Therefore, it is unclear which algorithmic technique was specifically used and whether it was perceived as machine learning after the deployment.

Under the same approach, AI system would not also be the Polish Syriusz – the system used for profiling the unemployed, as it only calculated the overall score of one's answers put in the questionnaire based on the values previously assigned to the answers.[12] This conclusion sounds surprising if one notes that Syriusz was indirectly mentioned in the other guidelines of the Commission as an example of detrimental or unfavourable treatment in unrelated social contexts prohibited under Article 5(1)(c)(i) of the AI Act.[13] It shall be noted that this functionality in Syriusz was abandoned after the second laws allowing its use were deemed unconstitutional.[14]

[10] *Ibid.*, p. 8.

[11] M. Wieringa, *Hey SyRI, Tell Me about Algorithmic Accountability: Lessons from a Landmark Case*, in *Data & Policy,* no. 5, 2023, p. 7, <https://doi.org/10.1017/dap.2022.39>.

[12] On the way how Syriusz system operates, see J. Niklas; K. Sztandar-Sztanderska & K. Szymielewicz, *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Fundacja Panoptykon 2014, p. 12.

[13] Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 4.2.2025 C(2025) 884 final, paragraph 57.

[14] The reason for the unconstitutionality of the provisions was the sub-statutory rank of the data processing norms, see Polish Constitutional Court judgment of 6.06.2018, K 53/16, OTK-A 2018, n. 38. I also write about this in: I. Gontarz, *Judicial Review*

However, from the description of the system's functioning, it appears it could be considered simpler traditional software based on the rules defined solely by natural persons.

Outside of the scope of the AI system definition would also be the system for registering notifications of tree felling in Estonia[15] or the system of automated exchange of data within the EU Settlement Scheme in the UK (if the UK decided to apply the AI Act).[16] These solutions are based on pre-coded, 'if-then' decision rules and databases, so they can't self-learn from the inputs. However, one could still argue that these are examples of the other approach to artificial intelligence referenced in recital 12 to the AI Act, namely «logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved».

As it derives from this analysis, it might be tricky for the external observer to determine whether the AI Act applies to a certain AI system. It follows that society might expect a higher degree of transparency on the algorithmic decision-making systems implemented, both in the aspect of informing about the systems as well as the technology implemented. Nevertheless, to the extent that the technological solutions used fall within the concept of AI systems, the Regulation constitutes a source of obligations for public administrations implementing or using such systems.

3. *Areas of high risk*

The main burden of obligations under the Regulation lies with providers of high-risk AI systems. Whether a system poses a high risk to security, health or fundamental rights is determined, in the context of public administration activity, by its ability to qualify for the areas listed

of Automated Administrative Decision-Making: The Role of Administrative Courts in the Evaluation of Unlawful Regimes, in *ELTE Law Journal*, n. 1, 2023, pp. 151-62, <https://doi.org/10.54148/eltelj.2023.1.151>.

[15] See in more detail paragraphs 39-40 of the reasons for the Judgment of the Supreme Court of Estonia of 28 September 2023, ref. 3-21-979, in which the court explicitly points out that the software technology used by the Environment Council is not based on machine learning.

[16] The principles of the aforementioned system are analysed in detail in: J. Tomlinson, *Justice in Automated Administration*, in *Oxford Journal of Legal Studies,* n. 4, 2020, pp. 718–27, <https://doi.org/10.1093/ojls/gqaa025>.

in Annex III to the Regulation.[17] In my view, there are at least 4 areas that cover public administration: 1) education and vocational training, 2) employment, 3) access to and enjoyment of essential public services and benefits, and 4) migration, asylum and border control management.

Firstly, in accordance with paragraph 3(a) of Annex III to the AI Act, AI systems intended to be used for the purpose of making decisions on access or admission to educational institutions and vocational training institutions or assigning persons to these institutions at all levels will be considered high-risk systems. The latter will, therefore, be by way of example based on Polish legal order, a system used by the Rector of a university in the context of an ongoing admissions process that results in an administrative decision.[18]

Secondly, according to paragraph 4(b) of Annex III to the AI Act, high-risk systems will also be AI systems intended to be used for the purpose of making decisions affecting the terms and conditions of the employment relationship, promotion and termination decisions, assigning tasks based on individual behaviour or personality or character traits, and monitoring or evaluating the performance and behaviour of persons in such relationships. Thus, a system whose operation is the basis for issuing a personnel order shaping an official relationship in the uniformed services (e.g. the Police, the Government Protection Bureau, the Central Anti-Corruption Bureau, etc.) should also be considered a high-risk system.[19] As in the case of education, no such system currently exists under the Polish legal system. However, it is worth mentioning that the evaluation of, for example, the performance of primary school teachers has been controversial in the US.[20]

Thirdly, according to paragraph 5(a) of Annex III to the AI Act, AI systems designed to be used by or on behalf of public authorities to assess the eligibility of individuals for essential public benefits and services, including health care, as well as to grant, reduce, cancel or claim reimbursement of such benefits and services, should also be considered high-risk systems. A high-risk system will, therefore, also be the one applied in social assistance matters by the executive bodies of local government units, as well as by the competent government administration. For example, the Polish

[17] Article 6(2) of the AI Act.

[18] The decision to refuse admission to a course of study referred to in Article 72(3) of the Polish Law on Higher Education constitutes an administrative decision within the meaning of the Polish Code of Administrative Procedure.

[19] Personal orders constitute administrative decisions.

[20] L. Dencik et al., *Data Scores as Governance: Investigating uses of citizen scoring in public services, Project Report,* Data Justice Lab, Cardiff University 2018, p. 11.

unemployment assistance profiling system or the Dutch SyRI system (if we assume that they constitute an AI system) could be assigned to this area.

Fourthly, the systems used in the area of migration management for security risk assessment or irregular migration and in processing applications for asylum, visas and residence permits, including the related assessment of the credibility of evidence, may pose a high risk.[21] This is where the voice recognition system for language tests used in ETS cases in the UK would have to be classified.[22]

One should note that, despite the AI Act mentioning a separate area concerning the administration of justice, no area would cover all the administrative proceedings in which administrative bodies decide about individuals. In my view, due to the authoritative concretisation of laws in a manner similar to the judicial application of the law, they could be listed in the last (8) area of Annex III. The risk to the right to good administration should be treated equally to the risk to the right to a court, which in its content expresses similar demands on the grounds of judicial procedure.[23]

Even if an AI system can be fitted into one of these areas, it does not have to comply with Section 2 of Chapter III of the AI Act as long as it does not pose a risk of harm to health, safety or fundamental rights.[24] This so-called 'extra layer' allows systems that do not significantly impact the outcome of the decision-making process to be taken out of the equation, either because a human performs most of the process or because the system only performs narrow preparatory or procedural tasks. In my view, the introduction of such a derogation is justified, but it may also lead to avoiding the

[21] Point 7(b) and (c) of Annex III to the AI Act.

[22] In these cases, automated decision-making included verification of the authenticity of the recording of the oral part of an English language test, designed to confirm knowledge of English at a sufficient level to live independently in the UK. Meeting this requirement was essential in the application process for a visa or indefinite leave to remain, see J. Tomlison; J. Maxwel, *Experiments in automating immigration systems,* Bristol University Press 2022, pp. 8-32.

[23] According to Article 41(1) of the Charter of Fundamental Rights of the EU: «Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union». According to Article 41(2) of the Charter, this right includes: the right of every person to be heard, before any individual measure which would affect him or her adversely is taken; the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; the obligation of the administration to give reasons for its decisions. On the matter of the standards of good administration see M. Princ, *Standardy dobrej administracji w prawie administracyjnym*, Wydawnictwo Naukowe UAM 2016, pp. 261-84.

[24] Article 6(3) of the AI Act.

application of the requirements of Section 2 of Chapter III of the AI Act to systems on which they should be imposed. Assessing the human factor in the decision-making process might be challenging, especially given the well-known automation bias phenomenon. Nevertheless, what could be assessed positively from the viewpoint of the protection of individuals is that the AI system is considered as of high risk always when it performs profiling of natural persons. Thus, the system provider will have to prove, i.a. that the system does not lead to discriminatory outcomes.[25]

4. *Key requirements related to automated administration*

Key requirements deriving from the AI Act may be considered from the viewpoint of the public body acting as the provider or the AI system or the deployer of it. The assumption that the system poses a high risk to security, health or fundamental rights will trigger the obligation for the provider (public administration body) to demonstrate that the tool meets the requirements of Section 2 of Chapter III of the AI Act.[26] These include, i.a. compiling technical documentation, demonstrating that the system complies with the requirements of the Regulation,[27] keeping records of events,[28] ensuring that the AI system is transparent to enable AI practitioners to interpret the results of the system and use them appropriately.[29]

Demonstration of compliance with these (and the other) requirements will be possible through a conformity assessment[30] based essentially on an internal audit (self-assessment - see Annex VI to the AI Act). The proof of the assessment is to be in the form of an EU declaration of conformity drawn up in writing by the provider and submitted to the competent national authorities upon request. From the viewpoint of public administration, there is no specific provision concerning public authorities

[25] Article 10(2)(f) of the AI Act.

[26] Article 16(a) of the AI Act.

[27] Article 11 of the AI Act.

[28] Article 12(1) of the AI Act.

[29] See Article 13(1) of the AI Act. The Regulation demands also putting in place a risk management system, including taking measures to address the risks identified [Article 9(2)(d)], the application of appropriate data management practices [Article 10(2)], ensuring human oversight [Article 14(1)], and designing the system to achieve appropriate levels of accuracy, robustness and cyber security [Article 15(1)].

[30] Article 16(f) in conjunction with Article 43(2) of the AI Act.

when it comes to AI system providers. In other words, public bodies are not subject to additional requirements when they act solely as high-risk AI system providers.[31] Nevertheless, some specific obligations are put on public bodies when they act as deployers.

At first, public bodies that are AI deployers are required to conduct a fundamental rights impact assessment.[32] This is an assessment analogous to a data protection impact assessment (hereinafter «DPIA»), nevertheless, the latter does not explicitly require an assessment of the influence against all fundamental rights.[33] Summary of the findings of the fundamental rights impact assessment carried out pursuant to Article 27 has to be published in the EU database.[34]

From the viewpoint of public administration activity, assessing the applied AI system against the right to good administration may be relevant. This right includes typical elements of due process, such as the right to be heard, the right of access to the file, and the obligation to give reasons for the decision. Therefore, if an assessment against the right to good administration is not performed as part of DPIA under the GDPR, the obligation will arise under the provisions of the AI Act.

It is also important to note that the fundamental rights impact assessment applies not only to processing personal data but to any processing within the AI system. Therefore, the AI Act seems to fill a certain gap that allowed AI to be applied by public administrations to, for example, business entities (commercial companies) without a proper assessment. A fundamental rights impact assessment will be produced as a result of an analysis of the operation of the system, and it may include the comments provided by stakeholders in the consultation.[35]

[31] It is worth to note that some additional powers and obligations are imposed on law enforcement authorities and public bodies acting in the area of migration.

[32] Article 27(1) of the AI Act.

[33] See Article 35(1) of the GDPR. «The reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion». See Article 29 Data Protection Working Party, 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, 17/EN, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, p. 6.

[34] As part of the information to be provided under Article 49(3) of the AI Act. See Section C of the Annex VIII to the AI Act.

[35] Although the duty to consult does not arise directly from the AI Act, it is mentioned in recital 96 to the Regulation. In my view, the opinion of the public should be mandatory, as part of democratic control, if the system is to be employed in administrative individual

Secondly, another modification vis-à-vis public authorities is the obligation to register their use of AI systems in the database. It should be noted that this is an additional requirement, as it is generally the provider's responsibility to register a high-risk AI system.[36] However, in the case of public authorities acting as deployers, they have to additionally notify the use of the AI system by attributing to themselves an AI system already registered in the database.[37] If public deployers establish that the high-risk AI system they intend to use is not registered in the EU database, they shall not use that system and shall inform the provider or distributor thereof.

This obligation should be strongly welcomed as encouraging transparency in the automation of administration. To date, there has been a lack of public registers of the systems used by public authorities. Own catalogues were created by social organisations or literature on the basis of the legal basis contained in legislation. However, these did not include systems that were used without a legal basis or were not disclosed by public authorities. This way, basic information about the system is made publicly available to AI users, addressees of AI system decisions and social organisations.

Both these requirements make an important contribution to ensuring that there is adequate documentation to prove the AI system's compliance with the Regulation. What is more, they enable social control over public administration activity by demanding transparency in the process of automating its activity. Interestingly, public administrations are required to adapt not only the high-risk AI systems that will be implemented after the Regulation's provisions enter into force but also those AI systems that are currently in use.[38] AI systems currently in use will, therefore, also have to be registered.

5. *Impact on the model of judicial review of public administration*

The control model adopted in the AI Act complements the existing model of judicial review of public administration's actions by assuming

decision making. However, even without mandatory consultations, fundamental rights impact assessment might be considered as an important tool to ensure transparency in the use of AI systems by public administrations.

[36] Article 16(i) of the AI Act.

[37] Article 26(8) in conjunction with Article 49(3) of the AI Act.

[38] See Article 111(2) of the AI Act. The systems have to be adopted to the requirements of the AI Act up to 2 August 2030.

prior verification of the AI system's compliance with the Regulation. It significantly resembles that of the GDPR. As with the processing of personal data, it covers the entire life cycle of an AI system, from its creation to its abandonment.

The verification is carried out as part of the conformity assessment, as a rule, by the provider.[39] Subsequently, each successive AI system operator is obliged to verify the proper fulfilment of obligations by the previous operator (e.g. an importer of an AI system in the event of suspicion of non-compliance of the system with the Regulation cannot place the product on the market). On the other hand, once the AI system is placed on the market, the market surveillance authority (hereinafter «MSA») supervises compliance with the AI system requirements.

It should be stressed that judicial review, which is, in the democratic state of the rule of law, the main pillar of the public administration control system, is only complementary under the AI Act. AI systems used by public administrations are mainly controlled by the public bodies (as AI providers) themselves and by the MSA, while only the decisions of the MSA are subject to action before an administrative court. Again, in this respect, the AI Act resembles the control model for the processing of personal data adopted in the GDPR, where the supervisory authority is primarily responsible for the institutional control over the processing of personal data, while the administrative court verifies the legality of the data protection authority's decisions.

An individual who has grounds to assume that the provisions of the AI Act have been breached may lodge a complaint with the MSA.[40] The latter may take this complaint into account for the purpose of conducting market surveillance activities. The filing of a complaint may, therefore, give impetus to the supervisory authority to exercise its supervisory powers and impose an administrative fine on the AI system operator (i.a. the public administration body). This complaint is not only available to persons whose legal interest has been violated but to anyone who considers that there has been an infringement of the provisions of the Regulation. Moreover, the AI Act does not apply only to the processing of personal data but to data processing in general. This is how the AI Act complaint differs from a complaint to a supervisory authority under Article 77(1) GDPR, being narrowed down to the data subject.

An individual aggrieved by the operation of a high-risk AI system can,

[39] As an internal control, see Article 16(f) in conjunction with Article 43(2) of the AI Act. For the rules of internal control see Annex VI to the AI Act.
[40] Article 85 of the AI Act.

therefore, realise his or her conventionally guaranteed right to a fair trial.[41] The automatic actions of the administration have not been taken out of judicial control, but a different form has been adopted for it – control of the actions of the market surveillance authorities. This solution seems appropriate, bearing in mind that in some European legal orders, such as the Polish one, administrative courts do not have the competence to conduct evidentiary proceedings, including the appointment of experts. On the other hand, specialised knowledge in the fields of IT, mathematics and data processing is required to be possessed by market surveillance authorities.[42]

6. *Space left to domestic lawmakers*

As an EU regulation, the AI Act produces legal effects directly in the national legal order and, unlike directives, does not require transposition by Member States. It, therefore, limits the regulatory autonomy of national legislators to the extent that the matter to be regulated has been harmonised.[43] The question thus arises as to what leeway is available to national legislators for automated administrative action. Has the AI Act exhausted the possibilities of making different assumptions to control the algorithms used by the administration? Since the Regulation aims to introduce a uniform legal framework throughout the EU, it would be impermissible, according to the principle of the primacy of EU law over national law, to adopt laws incompatible with its objectives.[44]

[41] Article 6(1) of the European Convention on Human Rights.

[42] According to Article 5(1) of the draft law on artificial intelligence systems, a new market surveillance authority under the AI Act is planned in Poland. This would be the Commission for Safety and Development of Artificial Intelligence. In my opinion, there are many arguments in favour of the aforementioned function being performed by a data protection authority. This is because it has the necessary expertise, adjudicating on data protection issues. It might be more economical to expand the existing authority instead of creating a new one. See Law on Artificial Intelligence Systems, project from 10.02.2025, Rządowe Centrum Legislacji, Projekt ustawy o systemach sztucznej inteligencji. Available at: <https://legislacja.gov.pl/projekt/12390551> accessed 4 April 2025.

[43] This follows from the principle of the primacy of the application of EU law, well established in the case law of the CJEU, see I. Gontarz, *Pierwszeństwo prawa Unii Europejskiej przed prawem krajowym. Kolizja z suwerennością na gruncie acquis communautaire i polskiego acquis constitutionnel,* in *Europa w 15 lat po wielkim rozszerzeniu UE*, Adam Mickiewicz University 2019, pp. 45-59.

[44] «Furthermore, in accordance with the principle of the precedence of community law, the relationship between provisions of the treaty and directly applicable measures of the

According to O. Mir, the rationale behind the AI Act was not to limit the institutional and procedural autonomy of the Member States. The researcher argues that the aforementioned values were the reason why it was not decided to adopt a common code of administrative procedure. He also refers to the scope of application of the right to good administration as expressed in the Charter of Fundamental Rights, the content of which omits national authorities, referring only to EU authorities. Finally, he also cites the provision of the AI Act allowing national law to be more relative to workers if the national legislator assumes that the guarantees contained in the AI Act are insufficient.[45]

I share O. Mir's view that the AI Act establishes minimum safeguards for the use of AI systems by public authorities, which cannot be reduced but can be strengthened by national lawmakers.[46] In my view, the European legislator does not regard administrative decision-making as an area of high risk since such a significant interference would undermine the institutional and procedural autonomy of the Member States. This is the consequence of assuming that the right to good administration enshrined in the Charter of Fundamental Rights applies explicitly only to European Union bodies, while national bodies are obliged to comply with this right when they apply EU law. At the same time, given that the AI Act already introduces concrete tools such as the EU database, creating parallel solutions may not be the most efficient solution.

Considering ways to supplement the AI Act's provisions, given some of the automated decision-making systems will not fit into the definition of AI system adopted in the Regulation, similar obligations could also be established on general automated decision-making by public administration. I am thinking in particular of the obligation to carry out a fundamental rights impact assessment, the documentation of which is

institutions on the one hand and the national law of the member states on the other is such that those provisions and measures not only by their entry into force render automatically inapplicable any conflicting provision of current national law but - in so far as they are an integral part of, and take precedence in, the legal order applicable in the territory of each of the member states - also preclude the valid adoption of new national legislative measures to the extent to which they would be incompatible with community provisions.», Judgment of the CJEU of 9 March 1978, Amministrazione delle Finanze dello Stato v Simmenthal SpA, Case 106/77.

[45] «It would make no sense that workers can enjoy more enhanced protection than that provided by the AI Act while citizens and legal persons dealing with public authorities do not», See O. M. Puigpelat, *The Impact of the AI Act on Public Authorities and on Administrative Procedures*, in *Fascicolo*, n. 4, 2023, p. 249.

[46] *Ibid.*, p. 4.

an important instrument for increasing the transparency of government action. However, a summary of the fundamental rights impact assessment results would have to be published in a separate national register to complement the EU database. Indeed, it would not be acceptable to register in the EU database systems that do not fall within the definition of an AI system. To effectively exercise social control, it is necessary to know about all automated decision-making systems used in the administration regardless of technology – not only AI systems. Therefore, an obligation to make such an assessment for any automated decision-making by the administration (not only based on machine learning) would benefit the ability to exercise democratic control over the administration.

Second, it is convincing to ban some AI system applications when dealing with individual cases, such as when there is a margin of appreciation. In my opinion, the abandonment of administrative discretion should result from the legislator's decision, preceded precisely by an impact assessment from the point of view of the right to good administration. It is also necessary to consider the principle of proportionality by balancing whether the abandonment of discretion will not disproportionately affect the sphere of individual rights and obligations. The AI Act leaves a gap in this respect, which could be filled by the national legislator along the lines of the German solutions.[47] Therefore, there is still some room for the provisions of the Regulation to be more specific about AI systems used by public administrations.

It is also worth bearing in mind possible changes to the AI Act itself. In this respect, it is worth considering extending the requirements for high-risk systems, such as the obligation to conduct a fundamental rights impact assessment and the obligation to register with the EU database, to all AI systems used by public administrations. This could be done by expanding the «justice and democratic processes» area listed in Annex III of the Regulation to «administrative decision-making processes». I believe such a measure would be justified by the similarity of the risks involved in both judicial and administrative types of law application. After all, in each case it is a matter of shaping the legal situation of a subject, on the one hand by a common court, on the other by a public administration body.

[47] See § 35a Verwaltungsverfahrensgesetz. See also the comments on the said provision from the perspective of Polish doctrine P. Rączka; S. Sasin, *Automation Of Administrative Acts: An Example Of The German Administrative Procedure Act,* in *Studia Iuridica*, vol. 102, 2024, <https://doi.org/10.31338/2544-3135.si.2024-102.10>.

7. *Conclusions*

In assessing the solutions adopted, it should be noted that the Regulation will significantly impact public administration bodies' activities. Despite the issuing of guidelines by the European Commission on the definition of AI systems, the latter still seems to raise questions in the doctrine. A broad interpretation of the concept of AI system should be postulated in a way that takes into account the demands of international organisations dealing with AI. Thus, AI systems should be considered, in my opinion, as systems with varying degrees of adaptability and even those without this capability (before or after deployment). Nevertheless, due to their reliance on traditional programming methods and simple algorithms, most automated decision-making systems used by public administrations will not fall under the provisions of the AI Act.

As providers of high-risk systems, public authorities will be obliged to demonstrate the compliance of implemented AI systems with the Regulation, maintain a risk management system, prepare technical documentation, and ensure appropriate data management practices, transparency, and human oversight. All AI systems developed in-house, procured, and simply used by public authorities will have to be registered in an EU database.

As deployers of AI, public authorities will be required to carry out impact assessments on fundamental rights, including the right to good administration. Together with the obligation to register the use of an AI system, the requirements placed on public authorities promote transparency in the automation of administrative activities and the exercise of public control over them.

The solutions applied to the administrative control model should be assessed positively. Indeed, the European legislator maintains the model adopted in the GDPR, under which the main control authority remains the supervisory authority, while its decisions are subject to judicial review. Thanks to such a solution, it is possible to ensure expert knowledge, while respecting the solutions of the Member States with regard to limited evidentiary proceedings before administrative courts.

Finally, it should be advocated that the AI Act has not deprived the national legislature of the space to regulate other automatic decision-making systems that do not fall within the scope of the AI Act. A mandatory fundamental rights impact assessment and its publication in a separate national register dedicated to automated decision-making

systems used by the administration would be useful. Secondly, the national legislator can still prohibit the automation of the handling of certain cases, in particular when there is a margin of appreciation. Some solutions could also be introduced into the AI Act itself, such as, for example, a separate high-risk area relating to administrative decision-making in general. In the context of dealing with individual cases, the absence of separate area concerning administrative decision-making in the Annex III to the AI Act, in my opinion, undermines compliance with the requirements of the right to good administration. What is more, there is no reason why national authorities applying EU law and other national authorities should be treated differently. They should all meet the same standards in terms of automatic administrative action, given similar requirements deriving from national codes of administrative procedure.

Afroditi Papathanasopoulou[*]

Social Media Companies' Duty under the Digital Services Act: Mitigating Disinformation Externalities while Protecting Freedom of Expression

1. *Introduction*

Over the past two decades, digital platforms have become the backbone of the online world, shaping both economic and social contexts. Social media, in particular, has been described as a 'double-edged sword'[1] generating both positive and negative externalities, i.e., effects of an activity or transaction that affect third parties who have no direct control over them.[2]

On the positive side, social media are crucial for communicating, acquiring and sharing information[3], and thus enhancing our fundamental rights, such as the freedom of opinion; access to information; and freedom of expression.[4] On the negative side, these platforms are increasingly

[*] PhD Student at Vrije Universiteit Brussel.

[1] E. Aïmeur et al., *Fake news, disinformation and misinformation in social media: a review*, in *Social Network Analysis and Mining,* vol. 13, no. 30, 2023.

[2] J. Tumlinson, *Externality,* in M. Augier; D.J. Teece (eds), *The Palgrave Encyclopedia of Strategic Management*, Palgrave Macmillan, London 2018, p. 546.

[3] *Ibid.*

[4] Article 19, *Regulating social media: we need a new model that protects free expression* in *Art.19.org*, 2018, <www.article19.org/resources/regulating-social-media-need-new-model-protects-free-expression/>.

associated with the spread of hate speech, fake news, disinformation and misinformation,[5] which undermine those same rights and freedoms, producing negative externalities in that sense.[6] Such negative externalities have intensified during major political, social, and health crises, including the 2016 U.S. presidential election, the COVID-19 pandemic, Brexit, and, more recently, the Russia-Ukraine war, the Israel-Hamas conflict, and the 2024 EU elections.

Unlike traditional media, social media content is produced and disseminated with minimal oversight, often by individuals lacking expertise.[7] Virality mechanisms, such as X's retweets and TikTok's algorithmic recommendations, further accelerate the spread of harmful content.[8] This has severe negative implications for individuals, posing a threat upon their fundamental rights and well-being. Fake news distorts reality, hampers the right to receive accurate information, and leads to self-censorship.[9] Such restrictions hinder individuals' right to freely develop their personality and participate in the social, economic and political life. At the broader social level, disinformation weakens public health and democratic processes. For example, during health crises, false news spreads misinformation about treatments,[10] while disinformation campaigns during elections manipulate public opinion and destabilise democratic institutions.[11]

Regulating these 'digital externalities' is essential to safeguarding fundamental rights and democracy. While direct state intervention in

[5] See for distinction: E. Aïmeur et al., *Fake news, disinformation and misinformation in social media: a review, cit.*; K.C. Ng et al., *The Effect of Platform Intervention Policies on Fake News Dissemination and Survival: An Empirical Examination*, in *Journal of Management Information Systems*, vol. 38, no. 4, 2021, pp. 898–930. In the present paper, fake news and disinformation are used interchangeably to denote intentionally false information designed to mislead the public.

[6] C. Diaz Ruiz, *Disinformation on digital media platforms: A market-shaping approach*, in *New Media & Society*, 2023, p. 9.

[7] K.C. Ng et al., *The Effect of Platform Intervention Policies on Fake News Dissemination and Survival: An empirical examination*, cit., p. 898.

[8] S.L. Myers, *How Social Media Amplifies Misinformation More Than Information: A new analysis found that algorithms and some features of social media sites help false posts go viral* in *The New York Times*, 2022, <www.nytimes.com/2022/10/13/technology/misinformation-integrity-institute-report.html>.

[9] S. Das, A. Kramer, *Self-Censorship on Facebook*, in *Proceedings of the International AAAI Conference on Web and Social Media,* vol. 7, no. 1, 2021, pp. 120-127.

[10] United Nations, *Hatred going viral in 'dangerous epidemic of misinformation' during COVID-19 pandemic,* in *UN News*, 2020, <news.un.org/en/story/2020/04/1061682>.

[11] S. Mckay, C. Tenove, *Disinformation as a Threat to Deliberative Democracy,* in *Political Research Quarterly*, vol. 74, no. 3, 2021, pp. 703-717.

content regulation is often seen as ineffective and undesirable, social media companies, as central gatekeepers of the digital sphere, bear significant responsibility for mitigating these harms.

This paper examines the regulation of social media externalities, particularly disinformation, by analysing the tension between self-regulation and government intervention. Focusing on the EU's approach under the Digital Services Act (Regulation (EU) 2022/2065- DSA[12]), it outlines key obligations imposed mainly on large platforms to combat disinformation and the challenges of content-restrictive powers as a restriction on free speech, including their limits under EU law. This paper also reviews the DSA's safeguards aimed at preventing excessive censorship and assesses whether these tools effectively protect freedom of expression, or if platforms' actions threaten this freedom.

2. *Regulating Digital Externalities*

Regulating platform governance is necessary, yet complex. The parties involved often struggle to negotiate on equal terms due to high transaction costs, power imbalances, and asymmetric information. For instance, while user trust drives social media market growth, platforms like Meta and X remain profitable despite reputational decline. This, combined with their dominant market positions, suggests that that market participants lack the power to effectively mitigate the externalities created by these platforms.[13] Additionally, digital market actors may have little incentive to combat disinformation and may even benefit financially from its rapid spread.[14] This market failure indicates the need for regulatory intervention.[15]

In principle, the state has a positive obligation to protect and uphold constitutionally guaranteed rights and freedoms of its citizens, yet regulating disinformation on social media poses several challenges. Policing content posted and disseminated through social media by state actors to detect and suppress such incidents is challenging, if not questionable, for several reasons. Firstly, besides its positive duty to protect fundamental rights, the

[12] Unless stated otherwise, all articles and recitals refer to the DSA.

[13] M.A. Cusumano et al., *Can self-regulation save digital platforms?*, in *Industrial and Corporate Change*, vol. 30, no. 5, 2021, pp. 1259–1285.

[14] C. Diaz Ruiz, *Disinformation on digital media platforms: A market-shaping approach*, cit., p. 2.

[15] *Ibid*, p. 9.

state also has a negative responsibility to refrain from activities that could potentially infringe on these rights. Direct state intervention in online content moderation risks violating freedom of speech, media freedom, and platforms' freedom to conduct business. Secondly, detecting misleading content is inherently complex due to the rapid spread of information, often driven by anonymous accounts and bots. States lack the necessary tools and access to address these issues effectively, whereas platforms possess the technological expertise, including big data, AI, and machine learning, to do so.[16]

Given these challenges, it is reasonable to argue that social media companies generating these externalities should be, in principle, the ones responsible for mitigating them. Policymakers are increasingly urging these companies to take the lead in reforming democratic governance on digital platforms.[17] The claim that these companies are merely neutral platforms with no influence over the content they host is undermined by their own business model. [18] Social networks primarily generate profits by selling advertisers access to predictive analytics derived from user data.[19] Thus, they reward what is most engaging, i.e. any content, factual or not, that generates clicks, likes and comments, thereby increasing user engagement.[20] They succeed this by constantly altering through algorithms and human intervention what is, and is not seen or recommended on their sites.[21] This control makes them central actors in shaping online interactions and information dissemination, though they differ significantly from

[16] W. Wolfs, J.J. Veldhuis, *Regulating social media through self-regulation: a process-tracing case study of the European Commission and Facebook*, in *Political Research Exchange*, vol. 5, no. 1, 2023, p. 18.

[17] Belfer Center and Shorenstein Center, *Democracy and Internet Governance Initiative: Towards Digital Platforms and Public Purpose*, in *Cambridge, MA: Belfer Center and Shorenstein Center*, 2023, pp. 10-12, <shorensteincenter.org/wp-content/uploads/2023/07/DIGI-Final-Report_July5_2023.pdf>; C. Diaz Ruiz, *Disinformation on digital media platforms: A market-shaping approach*, cit., p. 2.

[18] House of Commons Digital, *Culture, Media and Sport Committee, 'Disinformation and 'fake news': Interim Report: Fifth Report of Session 2017–19,* in *HC 363*, 2018, para 57, <publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf>.

[19] C. Diaz Ruiz, *Disinformation is part and parcel of social media's business model, new research shows*, in *The Conversation*, 2023, <theconversation.com/disinformation-is-part-and-parcel-of-social-medias-business-model-new-research-shows-217842>; D. Michaelis et al., *Media companies must reimagine their data for a digital world*, in *BCG Global*, 2017, </www.bcg.com/publications/2017/advanced-analytics-media-companies-reimagine-data-digital-world>.

[20] *Ibid*.

[21] House of Commons Digital, *Culture, Media and Sport Committee, 'Disinformation and 'fake news': Interim Report: Fifth Report of Session 2017–19,* cit., para 57.

traditional publishers,[22] who create, edit, and take responsibility for the content they share.[23]

To manage the externalities they create, social media companies can either self-regulate or be subject to government regulation.

2.1. *The Dilemma: Self-Regulation vs. Government Regulation*

Self-regulation does not imply deregulation but rather shifts regulatory responsibility from the state to industry actors,[24] leveraging industry's expertise in operations, standards, and best practices. Platforms, however, are primarily profit-driven, often lacking incentives to balance societal interests with shareholder gains.[25] Thus, regulating harmful content that threatens profits or increases costs is not their priority. They can however effectively become 'private regulators' of the digital space[26] by setting their own 'house rules' (e.g., Facebook's Community Standards), that define user activity limits and accessibility parameters.[27] The EU originally attempted to address harmful content through self-regulatory texts, such as the 2016 Code of Conduct on Countering Illegal Hate Speech Online[28] and the 2018 Code of Practice on Disinformation.[29]

Self-regulation offers a faster and more flexible approach compared to lengthy legislative processes, allowing industry experts to shape rules in line with corporate governance principles like 'comply or explain', rather than rigid legal provisions.

However, such rules often lack a unified approach and effective compliance systems. As recognised in the Sounding Board's assessment

[22] D. Bromell, *Regulating Free Speech in a Digital Age*, in Springer Cham, 2022, p.67.
[23] House of Commons Digital, *Culture, Media and Sport Committee, 'Disinformation and 'fake news': Interim Report: Fifth Report of Session 2017–19*, cit., para 57.
[24] M. Cohen, A. Sundararajan, *Self-Regulation and Innovation in the Peer-to-Peer Sharing Economy*, in *University of Chicago Law Review*, vol. 82, no. 1, 2017, p. 116.
[25] M.A. Cusumano et al, *Can self-regulation save digital platforms?,* cit., p.1263.
[26] *Ibid,* p.1266.
[27] M. Schröder, *A German Perspective on Self-Regulation of Online Platforms*, in *Journal of Law & Economic Regulation*, vol. 15, no. 2, 2022, pp. 7-23.
[28] The EU Code of conduct on countering illegal hate speech online <commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en>.
[29] Code of Practice on Disinformation <digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation>.

of the 2018 Code of Practice, the absence of a common approach, clear commitments, and strong compliance tools weakened its effectiveness.[30] The Commission acknowledged the shortcomings and reformed the Code in 2022[31] towards a more conduct-oriented version.[32] Additionally, self-regulation lacks democratic legitimacy, as it delegates regulatory power to private actors without adequate legal remedies.[33]

Without proper accountability, self-regulation proves inadequate, especially when compliance is costly and incentives are weak. Then, the threat of state-intervention serves as an external incentive for compliance[34], since it imposes legally binding obligations, enforced through penalties or incentives[35] that ensure positive externalities (e.g., patent rights) or mitigate negative ones (e.g., pollution taxes).

In the digital space, the EU has regulated various aspects of digital platforms, especially those with significant market power, through laws covering competition, consumer protection, and data privacy. To combat disinformation, the EU initially relied on self-regulation, allowing Member States (MS) to adopt their own approaches. While countries like Germany and France have enacted national laws, most preferred user awareness initiatives to avoid state censorship, while others solely relied on EU-level measures lacking national initiatives.[36]

Government regulation struggles to effectively address online harm as the costs of enforcement can exceed those of non-compliance, and tends to be slow and rigid due to legal requirements. As technology and business models evolve rapidly, regulation must remain flexible to avoid hindering platform innovation while ensuring legal compliance.[37]

[30] The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice, 2018, para 4, <ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456>.

[31] European Commission, *A strengthened EU Code of Practice on Disinformation*, <commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en>.

[32] S.M. Del Moral, *The DSA and the Fight against Online Disinformation in the Context of EU Law: Avenues for Internal Dialogue and External Territorial Extension,* in *Robert Schuman Centre for Advanced Studies -Centre for a Digital Society Working Paper RSC 2024/19*, 2024, p.16.

[33] M. Schröder, *A German Perspective on Self-Regulation of Online Platforms*, cit., p.11.

[34] M.A. Cusumano et al., *Can self-regulation save digital platforms?*, cit., pp. 1264-1265.

[35] *Ibid*, p.1262.

[36] F. Saurwein, C. Spencer-Smith, *Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe*, in *Digital Journalism*, vol. 8, no. 6, 2020, pp. 827-828.

[37] C. Bucsh, *Self-regulation and regulatory intermediation in the platform economy*, in M.

2.2. *The EU's Regulatory Approach: The DSA*

The EU recognising the limitations of both self and government regulation, opted for a hybrid approach combining state oversight with private sector 'social' responsibility to address misleading content online and platform governance. Despite arguments that major platforms are 'too big to regulate' due to their market power and technological complexity,[38] policymakers have pursued co-regulation, a mix of state supervision and industry self-regulation involving multiple stakeholders (e.g., advertisers, media, researchers, etc).[39] In this context, the Digital Services Act (DSA) alongside the Digital Markets Act (DMA) establish a supranational regulatory framework[40] that define platform accountability. The DSA, which became fully applicable across the EU on February 17, 2024, imposes harmonised obligations on digital platforms, ensuring user safety, fundamental rights protection, and enhanced content oversight. Particularly for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), stricter responsibilities aim to limit unsupervised private power while allowing platforms some discretion in establishing their terms of service (ToS). By holding platforms accountable to regulatory authorities while recognising their role in shaping the digital space, the DSA seeks to create a more transparent and accountable online environment.[41]

Cantero Gamito, H.W. Micklitz, (eds), *The Role of the EU in Transnational Legal Ordering,* Edward Elgar Publishing, 2020, pp. 115-134.

[38] A. Shephard, *The End of 'Too Big to Regulate': Facebook and other tech giants convinced politicians that oversight stifled innovation. That's all starting to change*, in *The New Republic*, 2018, <newrepublic.com/article/147642/end-too-big-regulate>.

[39] D. Stockmann, *Tech companies and the public interest: the role of the state in governing social media platforms*, in *Information, Communication & Society,* vol. 26, no. 1, 2023, p.3; C. Tan, *Regulating disinformation on Twitter and Facebook*, in *Griffith Law Review*, vol. 31, no. 4, 2022, p. 532.

[40] L. Bouza García, A. Oleart, *Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges*, in *JCMS: Journal of Common Market Studies,* 2023, p.5.

[41] M. Husovec, *Will the DSA Work? On Money and Effort*, in J. Van Hoboken et al. (eds), *Putting the DSA into Practice,* Verfassungsbooks, 2023, p. 21; C. Tan, *Regulating disinformation on Twitter and Facebook*, cit., p. 532; D. Stockmann, *Tech companies and the public interest: the role of the state in governing social media platforms,* cit., p.3.

3. *The DSA and the Regulation of Disinformation*

The DSA renders large social media companies the 'gatekeepers' of online content in upholding democratic values by introducing a binding legal framework across EU to tackle disinformation online and assigning liability to digital platforms.

Although disinformation is explicitly referenced only in the Regulation's recitals, the DSA introduces several obligations, especially for VLOPs to mitigate its risks, primarily by enhancing transparency and empowering users. Crucially, the DSA does not classify disinformation as illegal content, acknowledging its fluid and context-dependent nature across the EU.

Platforms are not required to proactively monitor all content but must review flagged material and take appropriate action. Failure to remove illegal content may expose them to liability under Art. 6. Thus, content moderation constitutes both a right and an obligation for platforms in addressing disinformation. VLOPs must assess systemic risks linked to their services, including how these services amplify false or misleading information, considering also local and linguistic differences.[42] They can mitigate risks by adapting their algorithms, improving authoritative information visibility, cutting ad revenue for harmful posts, or activating crisis protocols. The EC may also activate crisis protocols collectively, if necessary, to ensure the rapid dissemination of reliable information.[43] While the DSA encourages platforms to voluntarily adhere to codes of conduct, non-participation without sufficient justification may be considered when assessing compliance under the 'comply or explain' principle.[44]

Despite these measures, content moderation remains fraught with both practical and legal challenges. Algorithmic detection tools struggle to differentiate between harmful and legitimate speech, particularly in less widely spoken languages,[45] or when confronted with sophisticated manipulation tactics (e.g., bots, troll farms). Yet, manual moderation, though necessary, is inefficient at scale.

Additionally, global operation of platforms and legal fragmentation across MS complicates enforcement. Some jurisdictions deem disinformation

[42] Recital (84); Art. 34.

[43] Recitals (95), (108).

[44] Recitals (88), (104).

[45] D. Bromell, *Regulating Free Speech in a Digital Age,* cit., p.41; G. Canela et al., *Addressing Mis- and Disinformation on Social Media*, in T.D. Purnat, et al. (eds), *Managing Infodemics in the 21st Century*, Springer, Cham 2023, pp.118-119.

illegal, while others do not, leading to inconsistencies in how platforms regulate content. Moreover, under the DSA, only VLOPs must assess systemic risks, while smaller platforms are obligated to remove only illegal content. This creates conflicts, as content moderation policies depend on the national laws of the countries in which platforms operate and their own community rules. Consequently, content that is banned in one country may remain accessible in another, and material deleted from one platform may resurface elsewhere.[46]

Finally, content moderation raises concerns about freedom of expression, as over-enforcement may lead to censorship and restrict diverse viewpoints. The DSA requires VLOPs to assess these risks, but broad terms such as «negative effects on fundamental rights, civic discourse, or electoral processes» leave room for interpretation. This ambiguity, shaped by differing political perspectives, may result in the suppression of borderline content.[47]

4. *The DSA and the Right to Freedom of Expression*

4.1. *The right to freedom of expression*

The right to freedom of expression serves two parallel functions: individual empowerment and the integration of democratic society. Freedom of expression and access to information are universal human rights.[48] At the EU level, Art. 11(1) of the Charter of Fundamental Rights of the European Union ('the Charter') along with Art. 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) guarantee the right to freedom of expression, which includes the right to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. These articles are interpreted in the light of relevant case law of

[46] D. Stockmann, *Tech companies and the public interest: the role of the state in governing social media platforms,* cit., p.7.

[47] J. Barata, *The Digital Services Act And Its Impact On The Right To Freedom Of Expression: Special Focus On Risk Mitigation Obligations*, in *DSA Observatory,* 2021, <The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations - DSA Observatory (dsa-observatory.eu)>.

[48] Article 19 of the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966).

the European Court of Human Rights (ECtHR), which has affirmed that «freedom of expression is applicable not only to "information " or "ideas " that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population».[49] The ECtHR has developed principles to ensure, in practice, the effective protection of this right. Still, the interplay of opinions, the ad hoc circumstances, national historical and socio-political contexts, and technological advances continue to shape its case law.

4.2. *Social Media's Power to Restrict Freedom of Expression*

The EC, through the DSA, has established a principal-agent relationship by delegating certain powers to social media when restricting harmful or morally questionable content, which may directly impact free speech. This can be interpreted as either an expansion, protecting citizens from false or unsubstantiated information and fostering a safer online environment, or as a restriction on freedom of expression, limiting users from sharing information they consider relevant to public debate. According to Art. 6(1) of the Treaty on the European Union (TEU), fundamental rights are a source of primary law, and therefore all secondary legislation, such as the DSA, must fully respect and comply with them. Yet, delegating speech-restrictive powers to platforms is not unlawful from the outset, as freedom of expression is not an absolute right; it can be restricted under specific circumstances involving other conflicting interests.

Art. 10(2) of the ECHR and ECtHR jurisprudence permit restrictions that are prescribed by law, serve a legitimate aim, and are necessary in a democratic society. Similarly, Art. 52 of the Charter requires proportionality and adherence to public interest objectives or the protection of others' rights. Therefore, to be lawful, restrictions on speech must meet a three-part test: 1) any restriction must have a legal basis that justifies any limitations in a clear and straightforward manner *(principle of legality);* 2) it must serve legitimate objectives, such as protecting public interests or the rights of others, without harming the essence of the right *(principle of legitimacy);* 3) any restriction should be appropriate, necessary to achieve its objectives and proportionate stricto sensu, meaning that limitations do not impose disproportionate disadvantages relative to their aims and no less restrictive alternative would achieve the same objective *(principle of necessity*

[49] Case of Handyside v. UK App no. 5493/72 (ECtHR 7 December 1976), para 49.

and proportionality).[50] Mere discussion or dissemination of information, even if potentially untrue, does not automatically justify restriction, as this could unreasonably limit free speech depriving persons of the right to express their views and opinions.[51]

In the digital ecosystem, social media exercise private power over other private parties through content moderation policies, imposing private sanctions (e.g., deleting content, banning users) based on 'digital conduct' (e.g., sharing ambiguous information during COVID-19[52]). Such actions interfere with freedom of expression and may constitute 'prior restraints' under ECtHR case law. Regardless of their motivation, platforms exercise in principle legitimately their private power, given that fundamental rights have only an indirect horizontal effect, meaning that they do not create direct and independently enforceable legal obligations for private entities in the same manner as for states.[53] Platforms thus have broad discretion to develop and enforce their ToS, except where specific legal provisions (e.g., anti-discrimination laws) apply.[54]

The DSA mandates that platforms assess and remove flagged content through notice-and-action mechanisms, thereby enabling restrictions on users' freedom of expression when justified. However, the lack of a clear definition of harmful content allows platforms discretion in content moderation, resulting in the restriction of content not only when it is illegal but also when it conflicts with their policies.

The state itself cannot typically interfere with or influence a platform's decision to ban a user or restrict content. As interpreted by the ECtHR, Art. 10 of the ECHR does not require governments to provide access to private spaces for expressing views, provided alternative venues are available. In the *Appleby* case,[55] the ECtHR decided that freedom of

[50] Case C-336/19, *Centraal Israëlitisch Consistorie van België and Others* (2020) EU:C:2020:1031, para 64 and case-law cited.

[51] Case Of *Salov V. Ukraine* App no. 65518/01 (ECtHR 6 September 2005), paras 113-114.

[52] Case of *Smart Exit, Viruswaarheid and Plaintiff sub 3 v. Facebook* <ECLI:NL:RBAMS:2020:4966, Rechtbank Amsterdam, C/13/689184 / KG ZA 20-783 (rechtspraak.nl)>; Case of *Café Weltschmertz v. YouTube (Google)* <ECLI:NL:RBAMS:2020:4435, Rechtbank Amsterdam, C/13/687385 / KG ZA 20-650 CdK/BB (rechtspraak.nl)>.

[53] S. Theil, *Private Censorship and Structural Dominance: Why Social Media Platforms Should Have Obligations To Their Users Under Freedom Of Expression*, in *The Cambridge Law Journal*, vol. 81, no. 3, 2022, pp.645–672.

[54] *Ibid*.

[55] Case of *Appleby and others v United Kingdom* App no. 44306/98 (ECtHR 6 May 2003), paras 40-48.

expression does not guarantee access to specific private locations. Instead, access must be denied in a way that prevents people from effectively expressing their views or destroys the essence of their right to free speech. Regarding online platform liability, this case illustrates that users do not inherently possess a right to access a platform.[56]As long as they can turn to other platforms, users' freedom of expression is not, in principle, violated. However, often VLOPs hold dominant market positions and serve quasi-public functions rendering them akin to 'public spaces'[57]; thus, unjustifiably restricting access to these platforms may constitute a violation of the freedom of expression. Whether a platform meets such criteria requires a context-sensitive assessment,[58] including consideration of its broader corporate structure.[59]

4.3. *DSA's Content Moderation Obligations: A Risk to Free Speech?*

The DSA justifies platforms' power to restrict content as necessary to safeguard higher public interests (e.g., democracy, health) while protecting the rights and freedoms of others. However, the absence of clear definitions for 'disinformation' and what qualifies as a high-quality human rights impact assessment may lead to unintended consequences. This is particularly concerning when platforms handle borderline content.

Rather than establishing substantive rules defining legitimate versus illegitimate content, the DSA requires platforms to disclose content prioritisation and moderation decision-making processes. While these measures enhance user rights, they also place significant regulatory burdens on platforms, making them responsible for assessing reported content, balancing the relevant rights and interests, and determining the content's fate. Platforms may implement moderation at both the content (e.g., labelling false information) and the account level (e.g., a forwarding restriction or deprioritization policy on an account) within the limits of

[56] See case of *Stichting Smart Exit v. Facebook*, cit., where the District Court of Amsterdam citing ECtHR case law, emphasised that freedom of expression does not guarantee access to a platform of one's choice.

[57] See BVerfG, Order of the First Senate of 6 November 2019, 1-BvR-16/13-, para 88, <www.bverfg.de/e/rs20191106_1bvr001613en.html>.

[58] See the Federal Constitutional Court's Order of 22 May 2019, 1-BvQ-42/19, (ECLI:DE:BVerfG:2019:qk20190522.1bvq004219), para 15.

[59] S. Theil, *Private Censorship and Structural Dominance: Why Social Media Platforms Should Have Obligations To Their Users Under Freedom Of Expression*, cit.

Art. 23(1). The substantive protection of freedom of expression is thus left to a private entity.

The ambiguity of content moderation obligations under the DSA may lead to divergent enforcement approaches, each with distinct risks for freedom of expression. Certain platforms may interpret the DSA's requirements narrowly, removing only content that is explicitly illegal under national or EU law. In such cases, harmful but technically lawful content may remain unmoderated, given that platforms only bear liability when they play an active role in the communication of the infringing content or have actual knowledge of the illegal activity.[60] After the DSA's adoption, VLOPs with stricter responsibilities may need to reevaluate such permissive policies, as they risk non-compliance with the Regulation.

Conversely, due to the vagueness of new obligations (e.g., when platforms have 'actual' knowledge under Art. 6) and the risk of substantial fines for breaches, some platforms may adopt overly restrictive policies to avoid liability. This can lead to the over-blocking of lawful content,[61] creating a 'chilling effect' on free speech, potentially leading to undue censorship of political commentary, news, and controversial opinions.

Thus, platforms face a 'regulatory headache' in trying to comply with the new legal rules while avoiding free speech violations. The DSA acknowledges the risk of over-censorship and includes safeguards to prevent such outcomes. Otherwise, platforms could unilaterally dictate user rights, often through automated decisions lacking proper legal protections.[62]

4.4. *The DSA Mechanisms and Safe Harbors for Preventing Over-Censorship*

The DSA establishes procedural frameworks that delineate the legal principles governing the relationships between citizens and public-law entities within the EU. The application of these frameworks to typically private-law entities is justified by the DSA's entrustment of these entities

[60] Art. 4(1), 5(1) and 6(1); See also Joined Cases C-682/18 and C-683/18, *Frank Peterson v. Google LLC and Others and Elsevier Inc. v. Cyando AG* (2021) ECLI:EU:C:2021:503.
[61] See Case-401/19, *Republic of Poland v European Parliament and Council of the European Union* (2022) ECLI:EU:C:2022:297, Opinion of Advocate General Saugmandsgaard ØE delivered on 15 July 2021 (1) para 141.
[62] G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society,* Cambridge University Press, Cambridge 2022, p. 314.

with the protection of public interests,[63] and serve as quality control measures, guiding social media in balancing the right to free speech with the need for safety online. This means that, while not constitutionally bound to protect free speech, their public influence requires that content restrictions be based on legitimate grounds[64], and not just vague ToS clauses.[65] Consequently, any speech restrictive measure implemented through moderation policies, tools, or sanctions must meet the three-part test that translates into transparency, due diligence, accountability, and appeal mechanisms, that protect user's fundamental rights.[66]

Accordingly, the DSA does not impose a general obligation for proactive content surveillance (Art. 8), aligning with CJEU rulings[67] that such requirements could disproportionately infringe users' freedom of expression and privacy, as well as the hosting providers' freedom to conduct business. Instead, it outlines procedures and grants specific rights to users, such as the right to receive notifications, justifications for decisions, and the ability to appeal.

Art. 17 requires platforms to provide affected users with statements of reasons for moderation decisions, detailing minimum information requirements (**§**3) to safeguard users and prevent arbitrary content removal. These statements should be provided ex-ante, meaning not after user's request and be clear and easy to understand (**§**4).[68] Additionally,

[63] Case *Van Haga v. LinkedIn* <ECLI:NL:RBNHO:2021:8539, District Court of Noord-Holland, C/15/319230 / KG ZA 21-432 (rechtspraak.nl)>, para 4.14.

[64] S. Theil, *Private Censorship and Structural Dominance: Why Social Media Platforms Should Have Obligations To Their Users Under Freedom Of Expression*, n. 53; See also Case of *Café Weltschmertz v. YouTube (Google)* <ECLI:NL:RBAMS:2020:4435, Rechtbank Amsterdam, C/13/687385 / KG ZA 20-650 CdK/BB (rechtspraak.nl)>, para 4.10, where the District Court of Amsterdam ruled that YouTube's strict policy, permitting only WHO and RIVM-aligned content, was overly restrictive, given that blocking other critical content and allowing only these perspectives is inconsistent with the platform's role in public debate and democratic society.

[65] *Van Haga v. LinkedIn*, cit., para 4.23, where the District Court of North Holland concluded that removal of the profile was not done with due care, because the policy guidelines were not sufficiently clear about what could be classified as misinformation about Covid-19.

[66] D. Bromell, *Regulating Free Speech in a Digital Age*, cit., p. 89; Art. 14(4), 23 (3), and 35(1).

[67] Case 70/10 *Scarlet Extended SA v SABAM* (2011) ECLI:EU:C:2011:777; Case C-360/10, *SABAM v Netlog* (2012) ECLI:EU:C:2012:85, para 26.

[68] See the recent judgment of the District Court of Amsterdam (2024) <ECLI:NL:RBAMS:2024:3980, District Court of Amsterdam, 10767307 CV FORM 23-13934> para 17, where it held, in relation to the infringement of Article 17, that *'the*

these data should be submitted to the EC that maintains a public database to enhance oversight on content moderation policies.[69]

To strengthen users' rights, the DSA mandates a free-of-charge internal complaint-handling system, allowing users to contest moderation decisions and have their complaints reviewed under the supervision of appropriately qualified staff. If users remain dissatisfied, they can also utilise out-of-court dispute resolution mechanisms, providing an additional layer of protection against wrongful moderation (Art. 20-21).

As already discussed, the notice-and-action mechanism serves as a primary tool for addressing illegal content. To prevent, however, platforms from being overwhelmed by vague or abusive notifications, the DSA requires notifiers to submit precise and substantiated notices (Art. 16(2)). These provisions aim to filter out non-actionable reports, ensuring that only legitimate notifications trigger liability under Art. 6.[70]

Complementing these mechanisms, trusted flaggers, i.e., independent, expert entities vetted by Digital Services Coordinators (DSCs), play a central role in enhancing content moderation quality. Platforms are required to prioritise reports from trusted flaggers, who are expected to provide reliable, accurate and objective assessments (Art. 22). To ensure accountability, these entities must publish annual reports detailing their activities, including the content flagged, with repeated inaccuracies leading to status suspension or revocation.

For these mechanisms to be effective, proper transparency tools must be in place; otherwise, the internal organisation of social media companies concerning content moderation remains opaque, exacerbating information asymmetry. Accordingly, all online platforms must publish annual reports on their content moderation efforts (Art. 15), which include information about the handling of illegal content, use of automated tools, training measures, and complaints received. For VLOPs, these reports must be published semi-annually and must specify the human resources dedicated

mere reference to the Help Center in the email cannot count as such a notification. Thus, the requirements of Article 17(3) of the DSA or paragraph 4 of the DSA were not met in this e-mail. This information is not clear, easy to understand and in any case not in such a way that [the applicant] can exercise any rights of recourse to which he may be entitled'.

[69] Recital (66); Art. 24(5).

[70] Art. 16(3); see also Case C-324/09, *L'Oréal SA v. eBay International AG* (2011) ECLI:EU:C:2011:474, para 122, and Joined Cases C-682/18 and C-683/2018, cit., para 15 where the CJEU highlighted that vague or inadequately substantiated notifications should be considered when assessing whether providers have actual awareness of the illegality of specific disseminated information.

to content moderation, including their qualifications and linguistic skills, as well as accuracy indicators (Art. 42). Additionally, VLOPs must prepare reports on their mandatory systemic risk assessments, mitigation measures, and audit results.[71] They should also provide data access to regulators and vetted researchers (Art. 40) and engage independent auditors at their own expense to assess compliance with DSA obligations (Art. 37). These disclosure obligations of the DSA promote a culture of accountability within the digital ecosystem.

Ultimately, these provisions enable users and administrators to monitor platform activities and hold them accountable for any misuse of moderating powers. Key DSA provisions serving as safe harbours for platforms primarily include the liability exemption regime (Art. 4-6), which shields them from excessive liability for third-party content. The criteria for assessing whether platforms enjoy such protection include whether the network acts as a 'mere conduit' of a 'technical, automatic, and passive nature',[72] and whether it has 'actual' knowledge of specific illegal content.[73] Circumstances such as automatic indexing of uploaded content, the presence of a search function, and recommendations based on user profiles do not, in themselves, imply that the platform operator possesses specific knowledge of illegal activities or content circulated on the platform.[74] Finally, the 'Good Samaritan' clause (Art. 7) allows good-faith moderation without increasing liability risks, preventing platforms from either avoiding content review entirely or over-removing questionable material.

4.5. *Assessing the DSA Safeguards: Protecting Users and Curbing Disinformation*

Effective protection of basic rights requires robust procedural safeguards. While the DSA introduces such protections, their effectiveness is compromised if implementation is inadequate or if inherent weaknesses

[71] Art. 42(4), (5); N. Helberge, R.P. Samuelson, *The Digital Services Act as a Global Transparency Regime*, in *VerfBlog*, 2024, <verfassungsblog.de/the-digital-services-act-as-a-global-transparency-regime/>.

[72] Case C-324/09, cit., para 113; See also Joined Cases C-682/18 and C-683/2018, cit., para 109 where the CJEU noted that a platform using technology to detect potentially infringing content does not necessarily play an active role that grants it knowledge or control over that content.

[73] See Joined Cases C-682/18 and C-683/2018, cit., paras 113-116.

[74] *Ibid*, para 114.

in the legal text are exploited. Since restrictions on fundamental rights originate from EU law, it is imperative for the EU legislature to not only establish safeguards but also to clearly define their substance and ensure their enforcement. For instance, the DSA calls for 'reasonable' and 'proportionate' content moderation strategies that major platforms should adopt, but lacks clear definitions and criteria upon which the EC will assess the proportionality and legality of these actions.

Building on this concern, another inherent weakness within the legal text is found in Art. 20's lack of procedural standards, which gives platforms excessive flexibility in handling complaints, potentially leading to inconsistencies and overburdening out-of-court dispute resolution under Art. 21. This weakens the overall dispute resolution mechanism of the DSA, complicating effective enforcement and access to justice.[75]

Furthermore, the absence of uniform audit and transparency standards creates uncertainty for platforms and stakeholders. Adopting universally accepted auditing frameworks, akin to IFRS or GAAP financial auditing principles, would enhance consistency, comparability, and auditor accountability. While the Commission's Delegated Regulation on DSA audits offers a starting point, it remains insufficient.

Moreover, evaluating whether a user's freedom of expression is unjustifiably restricted should consider individual and contextual factors, making the lawfulness of disputed policies determined on an ad-hoc basis. A policy may not be unlawful in itself, but its application (e.g., indefinite or shadow bans) could violate freedom of expression. Thus, effective enforcement of the tools provided against platforms is crucial, as the law's efficacy hinges on willingness to comply and the ability of state agencies to enforce it.

Under Art. 49, each MS is tasked with supervising platforms based in their countries through designated DSCs in an impartial, independent, and transparent manner, while the EC oversees VLOPs under Art. 65. The EC has the authority to initiate investigations by requesting information, accessing data and algorithms, conducting interviews, and inspecting premises. If non-compliance is suspected, the EC can open formal proceedings and impose fines of up to 6% of global turnover. It may also apply interim measures to prevent serious harm to users and, as a last resort, seek the temporary suspension of services that consistently violate the DSA (Art. 67-74). Granting public authorities extensive supervisory powers is

[75] P. Ortolani, *If You Build It, They Will Come: The DSA's "Procedure Before Substance" Approach*, in *VerfBlog*, 2022, <verfassungsblog.de/dsa-build-it/>.

essential for state actors to fulfil their positive obligations under national and EU law, particularly in protecting free speech against abusive platform conduct. In this context, ex-ante control mechanisms are valuable, allowing proactive measures before lawful speech is censored.

The DSA designates the EC as the principal enforcer for large social media, which have stricter responsibilities. Consequently, the DSA endows the EC with broad investigatory powers, allowing access to platforms' operations and AI tools that would otherwise remain confidential. However, concerns have been raised regarding whether delegating these powers to the EC is the most effective enforcement solution, given that it also serves as the main executive body holding legislative initiative. This dual role makes the EC vulnerable to political scrutiny and control.[76] Therefore, it is argued that an independent body would be better equipped to enforce the DSA, ensuring accountability and ethical standards akin to those in the GDPR and EU media law.

Public enforcement must be complemented by enforceable rights and effective legal remedies for users to defend their freedoms against platform abuses, as the legality of content is determined by platform operators rather than state courts, making it essential for the DSA to empower users to enforce their rights against private entities. As noted, besides internal appeals, users may opt for an out-of-court dispute settlement body. Although this mechanism aims to protect users and alleviate the burden on courts, its effectiveness under the DSA remains questionable. Art. 21(2) only requires platforms to act in good faith and provide certain information, without obligating them to adhere to the out-of-court settlement body's decisions, as these are not binding. Consequently, users may still need to seek remedies from civil courts to uphold their rights, with high litigation costs posing a significant barrier for individuals seeking effective protection against large tech companies.

Art. 17(3)(f) of the DSA affirms users' right to judicial redress, while Art. 54 recognises private enforcement by allowing service recipients to seek compensation for damages or losses resulting from providers' failure to comply with the DSA. Whether compensation has a deterrence effect is yet to be seen. However, the terms 'damage' and 'loss' for wrongful moderation are not defined in the Regulation, leaving interpretation to national law. The concern extends beyond whether the DSA imposes direct obligations in favour of users to the nature of these obligations, whether they are

[76] I. Buri, *A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer*, in J. Van Hoboken et al. (eds), *Putting the DSA into Practice*, cit., p. 80.

obligations of means or obligations of results, as this affects platform accountability. The DSA primarily imposes obligations of means, focusing on platforms' actions and efforts rather than specific outcomes, such as establishing risk mitigation systems or taking reasonable measures to protect human rights, rather than completely eliminating harmful content. In any case, not adhering to the DSA's obligations imposed in favour of users means that the platform could be held liable not only for a breach of contract, but also for having acted unlawfully against them. In practice defending human rights seems to rely on courts interpreting platforms' ToS and due process safeguards, which may exceed the DSA's intended scope of reducing litigation and its associated costs.

It is true that courts, rather than private entities and non-independent bodies, can better assess whether a platform's approach aligns with the spirit of the DSA, which seeks to balance user safety with freedom of expression. In its *UPC Telekabel Wien*[77] judgment the CJEU emphasised that the right to an effective judicial remedy is essential for ensuring the exercise of freedom of expression online.[78] Judges are often better equipped to independently evaluate the lawfulness of speech and balance competing fundamental rights (e.g. freedom of expression and the rights of property and freedom to conduct business) under international and European human rights law (HRL), establishing legal precedent for distinguishing less obvious illegal or harmful speech that should be filtered.[79] Such precedents will, in turn, assist platforms, lacking legal expertise, in assessing the content posted and flagged on their services, informing the design of their content-filtering AI mechanisms, and establishing thresholds for their risk assessments on the impact on fundamental rights.

However, several factors should be considered regarding judicial redress: a) the rapid spread and varied nature of disinformation often exceeds the speed of legal rulings, leading to gaps in regulation; b) national courts interpret social networks' ToS and related content moderation decisions based on their own national legislation and cultural context. This can lead to divergent rulings across jurisdictions regarding the legitimacy of a platform's decision. Such variations in interpretation may complicate the uniform application of the DSA and hinder the consistent adoption of mitigation measures by VLOPs operating globally. Nonetheless, Art. 82(3)

[77] Case C-314/12 UPC Telekabel Wien (2014) EU:C:2014:192, para 57.

[78] Opinion of Advocate General, cit., para 179.

[79] *Ibid,* paras 197-199; O. Pollicino, *General Report: Freedom of Speech and the Regulation of Fake News*, in O. Pollicino (ed.), *Freedom of Speech and the Regulation of Fake News,* Intersentia 2023, p.38.

obliges national courts to refrain from making decisions that contradict those already adopted by the EC under the DSA; c) effective legal protection necessitates effective legal remedies, often in the form of injunctions as targeted monitoring measures with worldwide effects,[80] including bans on future legal violations from equivalent content, including by third parties.[81] Yet such injunctions have to be sufficiently specific and proportionately balanced against the platform's interest in avoiding obligations of general monitoring and taking disproportionate measures.[82] Otherwise, such requirements could overturn the exemption liability regime and establish a de facto general surveillance duty.

5. *Conclusion*

The spread of disinformation on social media poses a significant negative externality, threatening fundamental rights and democratic processes. Various actors, including platforms and institutions, are involved in both spreading disinformation and implementing countermeasures, such as content supervision. This creates a tension between protecting free speech and preventing it from undermining constitutional values or public interests.

Regulating these externalities is complex, as social media must remain open, and free. States have a dual responsibility: to protect fundamental rights by establishing adequate regulatory frameworks, while simultaneously avoiding actions that could unduly restrict rights, including

[80] See, however, Case C-376/22, *Google Ireland Ltd v KommAustria*, (2023) ECLI:EU:C:2023:835, para 34, where the CJEU in essence determined that the exception to the 'country-of-origin' principle in Art. 3(4) of the e-Commerce Directive prevents recent national content moderation laws from applying to service providers established in other countries.

[81] Case C18/18, *Eva Glawischnig-Piesczek v Facebook* (2019) ECLI:EU:C:2019:821, para 41, the CJEU held that for injunctions *'to bring an end to an illegal act and to prevent it being repeated, …must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. Otherwise, […], the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different […], which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim'*.

[82] C-18/18, cit., paras 44-47; Case C-484/14, *Tobias Mc Fadden v Sony Music* (2016) ECLI:EU:C:2016:689, paras 80-87; Case C-324/09, cit., para 131.

freedom of expression and platforms' rights to conduct business. Social networks must also maintain independence when acting as information communicators. Thus, platforms mut be responsible for managing the externalities they produce as they control algorithmic designs and ToS that shape what users see.

Platforms attempted to self-regulate by voluntarily adhering to industry-level codes of conduct. However, such soft-law instruments have proven inadequate due to their non-binding nature and inconsistent compliance. Government-led regulation alone is insufficient given the scale of digital platforms and the rapid evolution of online content, prompting the EU to adopt a hybrid approach through the DSA. This model holds platforms accountable while allowing for some self-regulation, recognising that one-size-fits-all solutions are impractical.

The DSA establishes a liability regime and grants platforms content moderation powers, which could lead to overly restrictive policies and wrongful moderation. To mitigate this, the DSA includes legal tools and safe harbours, such as: a) substantiated notices (Art. 16); b) clear reasons for content restrictions (Art. 17); c) trusted flaggers (Art. 22); d) transparency obligations (Art. 15, 24); e) auditing and reporting (Art. 37); f) risk assessments and mitigation measures for large platforms (Art. 34-35); and g) an exemption liability regime (Art. 4-6) along with the 'Good Samaritan clause' (Art. 7). It focuses more on procedural safeguards than on setting substantive content filtering rules, granting platforms wide discretion due to the absence of uniform standards and relevant case law. This approach is appropriate, given the ambiguity of the concepts at stake, the risk of arbitrary state intervention, and the rapid technological advances that demand flexible regulation.

For the DSA to succeed, two conditions are key: clear procedural rules for consistent enforcement and strong mechanisms to hold platforms accountable. The EC, with its broad investigative powers over large platforms, can monitor compliance and impose penalties. However, given the DSA's broader political and democratic implications, the EC's role in content moderation raises questions of institutional impartiality. Optimistically, alongside public enforcement, affected parties can seek redress through internal complaint mechanisms, out-of-court resolutions, and state courts. These avenues, especially judicial redress, enable individuals to challenge arbitrary decisions by private actors, who often lack the expertise to interpret content moderation cases through the lens of international and European HRL. Judicial oversight also generates

legal precedents that can guide future platform practices. Nevertheless, litigation remains lengthy and costly, which may limit its accessibility as an effective remedy. Thus, relying solely on traditional mechanisms may be insufficient to resolve the tension between online disinformation and freedom of expression.

Ultimately, the effectiveness of the DSA will depend on how its mechanisms are implemented, how obligations are enforced, and how stakeholders collaborate to address these complex challenges. Ensuring that transparency obligations function effectively will be critical in preventing behind-the-scenes interactions that could undermine content moderation neutrality. Still, much remains to be seen regarding the future of the Regulation and its impact on safeguarding both freedom of expression and the fight against disinformation.

Anastasia Nefeli Vidaki*

Blockchain for Criminal Justice in the EU: an Opportunity or a Threat?

1. *Introduction*

Over the past years, technology has flooded every part and parcel of our everyday lives. This unprecedented wave became more sweeping during the COVID-19 era, which forced even the more hesitant individuals, countries, and organisations to begin, continue, or enforce their digitalisation procedures. AI, the Internet of Things (IoT) became vastly utilised, applied, and more specifically regulated. A pre-existing technological tool, thus, which was present and thriving before the digitalisation fever, mainly in finance and transactions, was blockchain. Encryption technology, a core part of blockchain, has proven to be the cornerstone of network innovation and information processing, serving as the basis of the Fourth Industrial Revolution.

Blockchain used to be severely marginalised in the financial sector, and its potential for expansion to other sectors was overlooked for quite some time. The fact that its application is not limited to the industry or that the industry itself is integrating fields traditionally driven by public authorities signifies a paradigm shift. Furthermore, its mention in the European Union (EU) policy documents has relatively recently revived the conversations regarding its usage, which, unfortunately, have not gained traction at least within the western part of the globe (EU and US). It has been argued that

* PhD student at Vrije Universiteit Brussel.

the future of law enforcement, crime management, and criminal justice will be based on the cloud, driven by machine learning, big data, and managed by AI; all of which will be built on distributed, encrypted, tamper-resistant blockchain networks.[1] That might sound like science fiction at first glance, but taking into account the fact that new crimes emerged during the early days of the internet boom, and the inadequate and insufficient response of criminal justice to them, attention should be drawn to the evolving investigation patterns and judicial measures led by new technologies.

As a result, literature on the possibility of such a utilisation, addressing its use cases, its benefits, and the concerns it might raise, as well as ways to tackle them successfully, especially from a legal and ethical perspective, is rather poor. The existing paper aims to provide some initial thoughts about this prospect to conclude whether it will be seen as a blessing or a curse for the EU. It begins with an attempt to define blockchain as prescribed in the policy documents and to explain the characteristics that reinforce its application in criminal justice. It continues by explaining the current situation of its usage in criminal justice and investigation across the world, with a focus on China, where it is widely applied. Following the criminal procedure, it examines the cases in which blockchain can be used, namely for update and verification purposes of warrants, evidence either physical or digital, judicial decisions, and criminal records at every single moment of the process; from the beginning of the preliminary investigation till the publication of the verdict and in some circumstances even after it. By elaborating on these scenarios, in this paper, the benefits of this technology for the involved parties in criminal justice and its more questionable parts can be spotted, for the successful confrontation of which we propose some alternative solutions. The research concludes with some remarks on the findings and calls upon the reboot of the talks on a European and international basis with the vision towards a future where blockchain is lawfully and ethically integrated into criminal justice.

[1] S. Williams, M. Maureen, *What Blockchain Means to the Justice and Public Safety Sector*s, in IBM Supply Chain and Blockchain Blog, 2019, <https://www.ibm.com/think/topics/blockchain-for-public-safety>.

2. *Judicial Blockchain*

2.1. *Definition*

Blockchain has been put under the umbrella term of Distributed Ledger Technology (DLT) and defined as a peer-to-peer, decentralised network structure,[2] comprised of blocks, namely digitally recorded data linked together in chronological order into one chain. Once the block of data is chained to the already existing data on the blockchain, it cannot be altered without changing all subsequent data blocks. Thus, this would require collusion from most of the network's computers.[3] The EU defines blockchain as «*a technology that allows people and organisations to reach agreement on and permanently transparently record transactions and information without a central authority*».

Although the importance of blockchain has been stressed in several policy documents produced by its institutions, the EU remains hesitant in realising numerous blockchain applications. However, it has been recognised that the potential of blockchain technologies goes beyond the strictly financial sector and that there is a growing number of use cases outside of it. New technological notions such as decentralisation, interoperability, and efficiency have gained ground in our everyday lives. Therefore, justice and law enforcement, in general, would not be able to escape from this unprecedented breakthrough.

The traditional belief that the judiciary should focus plainly on the correctness of each judgment and turn a blind eye to the matters of duration or costs has gradually given its place to a novel perception, according to which time effectiveness and affordability of the costs play an important role and should be balanced with the need for correct, solid and fair procedures and decisions. This considerable change has not only occurred in the administration of justice but also in law enforcement.[4] The expansion of the internet and the shift of crime from the tangible sphere into the digital,

[2] J. Herbert, A. Litchfield, *A novel method for decentralized peer-to-peer software license validation using cryptocurrency blockchain technology*, in Proceedings of the 38th Australasian Computer Science Conference, ACSC 2015, <http://crpit.com/confpapers/CRPITV159Herbert.pdf>, pp. 27.

[3] J. Salmon, G. Myers, *Blockchain and associated legal issues for emerging markets,* in International Finance Corporation Note, 2019, pp. 63.

[4] R. Assy, *Briggs's online court and the need for a paradigm shift,* in Civil Justice Quarterly, no. 36, 2017, pp. 21.

intangible world calls upon agencies involved in the battle against criminal behaviour to be equipped with trained personnel and to utilise up-to-date techniques, capable of keeping up with technological progress. Although civil justice has been influenced too, criminal justice, which demands the cooperation of the judiciary and law enforcement agencies, constitutes the primary judicial branch in which blockchain could be introduced, applied under specific conditions, and release its full potential.

In the e-justice 2019-2023 Action Plan, the EU states its vision to incorporate innovative technologies in criminal justice cross-border judicial cooperation processes. Along with AI and robotics, blockchain appears among the proposed projects.[5] Although the integration of AI and robotic systems into the judiciary seems to be clearer, the use of blockchain technologies for its procedures remains a slightly unexplored field in the EU. The business sector follows another path since startups innovating to bring blockchain closer to law enforcement are blooming.[6] This is not the case in other countries, where discussion has been converted into action and blockchain has gradually been integrated into the judicial system.

In the United States (US), another dominant country in emerging technologies, the discussions on the possible use of blockchain for the judiciary started some years ago, and tech companies have been engaged in launching blockchain-based management systems for criminal records and evidence. Until now, except for those private initiatives, no measure has been adopted on a federal level regarding the introduction of blockchain to criminal justice or criminal investigation.

By contrast, China has made notable institutional advances. Since 2018, its judiciary has incorporated blockchain within a national legal framework. The Supreme Court of China authorised the use of blockchain for judicial purposes, notably within the Internet Courts, a system in which legal proceedings are conducted entirely online (Hangzhou Court Network, 2018).[7]

The Hangzhou Internet Court launched the country's first national judicial blockchain platform, a consortium connecting local court blockchains to form a unified system for managing and verifying evidence. This platform consists of thirteen nodes, including courts, notary offices, and technology partners such as the Judicial Appraisal Institute of the

[5] European Union, 2019-2023 Action Plan European e-Justice. ST/5140/2019/INIT, OJ C 96, 13.3.2019, pp. 9–32.

[6] ND. *Banking is only the beginning: 58 big industries blockchain could transform CBInsights,* 2022, <https://www.cbinsights.com/research/industries-disrupted-blockchain/>.

[7] Hangzhou Court Network, *Introduction to the Hangzhou Internet Court*, 2018, <http://www.zjsfgkw.cn/col/col280/index.html>.

Shanghai Computer Industry Association, the Qiantang Notary Office, and Ant Financial Services. While this setup enhances traceability and tamper resistance, the unclear distribution of public versus private control over the nodes has raised concerns about transparency and governance.[8]

Furthermore, in Foshan, blockchain has been deployed in the surveillance of parolees, where offenders are monitored via electronic bracelets that transmit tamper-proof data in real time.[9] This pilot illustrates the breadth of blockchain's utility, from courtroom procedures to offender management.[10]

2.2. *Use Cases of Blockchain in Criminal Justice*

While the EU has endorsed blockchain as a strategic digital priority, its normative framework for blockchain use in criminal justice remains embryonic and fragmented. The aforementioned soft-law instruments might acknowledge blockchain's transformative potential, but stop short of articulating binding regulatory or ethical standards specific to criminal procedure. From a normative perspective, this lacuna is problematic. Criminal justice systems require guarantees of legality, accountability, and proportionality, all of which are underdefined in current EU blockchain discourse. As Finck argues,[11] the EU's legislative instruments are often technology-neutral, but neutrality is not normatively sufficient in domains where rights, such as due process and privacy, are structurally at risk. Without a clear delineation of legal responsibility for smart contracts, data immutability, and access permissions, blockchain risks becoming an opaque layer over an already complex system. Thus, the EU's current blockchain

[8] G. Du, M. Yu, *When blockchain meets electronic evidence in China's internet courts*, 2021, <https://www.chinajusticeobserver.com/a/when-blockchain-meets-electronic-evidence-in-china-s-internet-courts>.

[9] S. Scott, *Blockchain behind bars: The case for cryptocurrency in criminal justice,* in Harvard Technology Review, 2021, <https://harvardtechnologyreview.com/2021/08/28/blockchain-behind-bars-the-case-for-cryptocurrency-in-criminal-justice-2/>; M. Francis, *Blockchain as best practice: The benefits of the criminal justice system implementing blockchain technology*, in Journal of Law and Technology. University of Richmond, 2022, <https://jolt.richmond.edu/2022/01/06/blockchain-as-best-practice-the-benefits-of-the-criminal-justice-system-implementing-blockchain-technology/>.

[10] Internet Law Watch., *The nation's first judicial blockchain: the underlying system of future litigation has been paved*, 2018, <https://zhuanlan.zhihu.com/p/44861173>.

[11] M. Finck, *Blockchain Regulation and Governance in Europe*, Cambridge University Press, 2018.

agenda, though progressive in rhetoric, requires substantive normative scaffolding to ensure it upholds the constitutional values and fundamental rights embedded in the EU acquis. A criminal justice-specific framework must move beyond pilot enthusiasm to address the constitutionalisation of digital infrastructure in adjudication and enforcement.

Despite the hesitation of the EU to involve blockchain in the core of justice, some aspects of the administration of criminal justice would be highly advanced by the involvement of this technology. Before proceeding with exploring each field of the criminal procedure in which blockchain could be involved, it is essential to clarify that the term blockchain for judicial or law enforcement purposes is not a public one, but rather a consortium one. A consortium blockchain is a type of blockchain that is created and managed by a group of organizations working together for a specific purpose.[12] Those consortium blockchains could be expanded from the preliminary investigation to case management till the court phase,[13] being inextricably linked with the whole criminal justice procedure.

2.2.1. *Warrants*

Indisputably, a criminal investigation in most jurisdictions is initiated with the issuance of a warrant, which simultaneously sets the starting point of the criminal procedure. Normally, courts or prosecutors are responsible for issuing search and arrest warrants to enable different law enforcement agencies to proceed with their duties. Police, parole, or probation officers need access to the warrant and are often asked to check its validity by contacting the issuing authority. In the EU, the European arrest warrant, a simplified cross-border tool for the prosecution or execution of a custodial sentence or detention order, makes the whole process even more complicated, as various agencies from various states might need to be involved.[14] At the same time, further information on the investigation should be added on their side to the already-existing warrant. The big and sometimes unclear number of participants and handoffs, the urgent need for updated information that does not, though, violate the integrity of the warrant, and for real-time record-keeping make it the ideal field for the

[12] A. Baliga, *Understanding blockchain consensus models*, in Persistent, 2017, <https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf?_ga=2.21200635.1919538867.1522092864-1798624458.1520283070&source=post_page>.

[13] F.C. Tsai, *The application of blockchain of custody in criminal investigation process,* in Procedia Computer Science, no. 192, 2019, pp. 2782.

[14] European Commission. (2017). Commission notice — Handbook on how to issue and execute a European arrest warrant. OJ C 335, 6.10.2017, pp. 1–83.

deployment of blockchain technology.[15]

By determining courts, prosecutors, criminal history repositories, and police officers as the nodes of a blockchain network, each of them individually and without prior authorisation of the other would have access to the criminal charges and would be in the position of updating the single blockchain record with the actions they took. Criminal charges on the initial blockchain record would flow intact throughout the whole adjudication process, tying actions of the involved parties and charges pressed upon them. This would allow all of them to keep track of the progress of a criminal investigation, to check the involvement of each agent, and to evaluate its lawfulness in the end.

2.2.2. *Evidence*

The management of forensic evidence, particularly in the chain of custody, which refers to the process of recording the state of evidence in chronological order during a criminal investigation, constitutes a crucial matter in the criminal justice system. In the era of the internet, crimes have transitioned from the analogical to the digital reality, and the same can be observed with the evidence. Compared to traditional evidence, digital evidence, consisting of sensitive data, is far more vulnerable, as it is easier to copy, transmit, modify, and contaminate.

Criminal justice is organised in levels and phases, the charge of which is different agencies each time. The collected evidence should remain accessible to all and unaltered throughout the whole procedure. The integrity of the chain of custody is vital to ensure that the evidence presented in the courtroom is reliable and untainted. Failure to follow the proper chain of custody procedures might result in the presentation of forged evidence and, in the long run, wrongful convictions or acquittals. It is necessary that at the chain of custody, evidence is documented at every stage of the investigation process, from its acquisition, collection, and analysis, and that the competent units deliver it to the laboratory, along with information on the time, place, cause, and manner of use of the evidence. Taking into account the significance of chronological order for purposes of proof of facts in legal proceedings, recording timestamps are necessary.[16] To avoid errors in the chain of custody and to maintain

[15] D. Graski, P. Embley, *When might blockchain appear in your court?* National Center for State Courts, 2018, <https://www.ncsc.org/__data/assets/pdf_file/0018/14913/blockchaininthecourts.pdf>.

[16] Tsai, *The application of blockchain of custody in criminal investigation process,* cit., pp. 2780.

the fairness of the judicial processes, it is important to agree upon and implement clear guidelines for the handling and preservation of evidence. Lack of their establishment would erode public confidence in the criminal justice system and jeopardise the rights of those caught up in it.

Under the above, it becomes evident that the chain of custody in criminal cases would greatly benefit from an integration of blockchain technologies. Since current evidence management systems are prone to theft, tampering, and, in the worst-case scenario, manipulation of the evidence they entail by the system itself, there will be dramatic improvements in the integrity of a chain of custody if the evidence is recorded on blockchain technology. At the time of the submission of evidence to police custody, the officers would be asked to report the current status of the evidence. After that, any agent altering in any form the evidence would have to confirm that it was in the same state as captured on the blockchain in the first place. Then, any person receiving the evidence in a chain of custody could directly compare the state of the evidence as initially reflected in the system with the state lastly recorded on the blockchain. If the evidence appears to have been violated, the recipient may refuse to accept it and proceed with an immediate report of the problem, rather than simply accepting it unaware of the state of the evidence when it was first placed in the chain of custody. The same could be done by any individual accused of a crime at the trial stage. They would be able to compare the evidence collected at the crime scene with the previously recorded status of the evidence on the blockchain.[17] As a consequence, blockchain can provide a tamper-resistant method of documenting and sharing (on a public or private basis) the custodial chain, evidence, and assets, which could contribute to a reduction of loss, theft, and misappropriation and an increase of transparency and accountability.[18]

In police investigations, blockchain might appear as an important tool for the use of evidence gathered by law enforcement authorities. As long as the maintenance of the integrity of the chain of custody is of paramount significance, a distributed, hard-to-forge record via blockchain could offer an extra level of security to the evidence-handling process and ensure that it has not been altered or processed in any way, eliminating the chances

[17] D. Anderes, E. Baumel, C. Grer, R. Veun, S. Wright, *The use of blockchain within evidence management system,* <https://f.hubspotusercontent10.net/hubfs/5260862/Ebooks%20and%20Whitepapers/Blockchain%20of%20Evidence%20FINAL%20DRAFT-3.pdf>.

[18] Williams, Maureen, *What Blockchain Means to the Justice and Public Safety Sector*s, cit.

of evidence falsification.[19] Blockchain can be used at an earlier stage to identify certain criminal financial activity patterns, giving the police a warning when an individual is involved in suspicious transactions, serving crime prevention. All in all, both at the investigation and at the trial for suppression or even for prevention purposes, blockchain technology can be used as a tamper-evident and tamper-resistant way to collect, structure, present, store, and secure data serving as evidence.

In front of the new e-evidence legislative package,[20] new obligations arise for the member states, where blockchain might be able to assist. The Regulation would allow an authority of a member state to request directly from a service provider to produce or preserve electronic data needed for the investigation and prosecution of crimes, introducing two new investigative measures: the European production order and the European preservation order.[21] The Directive would require service providers to designate a legal representative in at least one member state as a contact point in charge of receiving and enforcing orders issued by competent authorities from across the EU.[22] Blockchain could be introduced in both procedures and legislative instruments, allowing all participants to follow the orders from their issuing till the finalisation of the investigation, to exchange data securely through it, and to integrate the legal representative of the service providers as the initial nodes, responsible to upload on it the evidence they are asked to.

2.2.3. *Judicial Decisions*

In the core part of judicial procedure, the resolution of a dispute before a court and the production of a decision, blockchain has not penetrated yet. Thus, two conceptual avenues for its integration have emerged. The

[19] S. Trendall, *UK Ministry of Justice talks up potential benefits of blockchain for the criminal justice system,* 2017, <https://www.holyrood.com/news/view,uk-ministry-of-justice-talks-up-potential-benefits-of-blockchain-for-the-criminal-justice-system_7876.html>.

[20] European Parliament. (2023). Legislative resolution on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD)).

[21] European Parliament & Council of the EU. (2023). Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Council document PE-CONS 4/23 of 2023-06-15.

[22] European Parliament & Council of the EU. (2023). Directive laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. Council document PE-CONS 3/23 of 2023-06-15.

first, and less invasive, involves using blockchain to update and synchronise judicial decisions beyond the confines of a single courthouse, allowing appellate courts or legitimate stakeholders to access the most recent authoritative version of a judgment. Regardless of how many third-party data aggregators or courts have interacted with the case, a blockchain-based record could ensure that only verified and updated information circulates among those who have a legitimate interest.[23]

The second, more speculative, model contemplates replacing or supplementing aspects of adjudication with automated, algorithmically managed systems. While the idea of fully automated justice may appear dystopian, pilot projects in civil and commercial arbitration have explored blockchain-based resolution mechanisms. In such systems, disputes are routed to digital arbitration panels, with parties incentivised through cryptocurrencies to act fairly. However, any implementation of such a system within the EU must respect privacy and procedural safeguards. To provide a fair and just resolution of the dispute, the platform should also be equipped with mechanisms for appeals and allow the parties to pursue their case before the court of law if they decide to do so. A prerequisite would be that all parties involved in this blockchain-based dispute resolution have beforehand consented to it after being fully informed about the procedure and its effect on their rights and claims. This relatively inexpensive, swift, and transparent system would be a nice alternative to an extensive, tiring time and cost-consuming pleading of a case before a traditional court.[24]

While such technologies may offer efficiency gains, they must operate within a rights-based legal framework that ensures the rule of law is not compromised by technical innovation.

2.2.4. *Criminal Records*

Nowadays, criminal justice partners use mostly manual data entry, ongoing audits, and quality-control efforts to maintain the databases for criminal records. Prosecutors, courts, and criminal history repositories are all responsible for updating criminal charges, which can usually cause confusion or lead to incorrect inputs. In criminal justice, where a single mistake would mean the false accusation, conviction, or incarceration of an individual, the need to vanish or at least to diminish this possibility

[23] Graski, Embley *When might blockchain appear in your court?*, cit, pp. 28-32.

[24] European Union Blockchain Observatory. (n.d.). Governance of and with blockchains. Retrieved from <https://www.eublockchainforum.eu/reports/governance-and-blockchains>, pp. 23.

becomes more urgent than ever.[25] But, with blockchain technology, the courts, prosecutors, and law enforcement officers could modify the initial blockchain-run criminal record, pass it throughout the whole criminal procedure, and possibly after it to the rest competent agencies who are legally granted to access it. Every time an amendment is conducted, the blockchain records the party who made it. Another important feature is that only individuals who have been delegated such authority ad hoc would have the ability to make alterations. For the electronic exchange of information between EU member states on offenses and convictions, the European Criminal Records Information System (ECRIS) has been established.[26] Its common communication infrastructure, operated with an encrypted network based on national criminal record databases could be enhanced by blockchain technologies.

3. *Benefits of the use of judicial blockchain*

To this day, law enforcement agencies do not share common databases in most countries, with each of them holding a separate one, which poses serious obstacles to the fluidity of data flow between them. This increases the fear of communication problems, technical malfunctioning during common investigations, and mishandling of the involved evidence. The risks of intransparency, forgery, or cyberattacks, and violation of the right to a fair trial following an unlawful investigation remain present. Blockchain promises to merely solve some of those thorny issues thanks to its immutable, decentralised, dispersed, and transparent nature.

3.1. *Immutability*

Blockchain data is represented as blocks in a sequence, making new data irrevocable. Each data point added is a new block that references its predecessor. A change is, therefore, impossible as all blocks are connected. Blockchains are designed so that data, once written to the chain, cannot be changed, erased, or rewritten. By employing blockchain at all the phases

[25] Anderes, Baumel, Grer, Veun, Wright, *The use of blockchain within evidence management system,* cit.

[26] Council of the EU, Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA. OJ L 93, 7.4.2009, pp. 33–48.

of criminal proceedings, the distributed ledger will remain unchanged. It is commonly accepted that preventing the tampering or contamination of evidence, especially digital evidence, is vital to ensure its legal defensibility. The blockchain ledger ensures that no single party gains control over the peer-to-peer network, which reduces the danger of data corruption. Its cryptographic security provides an extra layer of protection against data manipulation. Additionally, this technology can provide real-time access to the evidence and necessary information linked to the chain of custody. This means that authorised parties can access the records at any time, managing and monitoring evidence throughout the entire legal process. They can save time and resources while ensuring the integrity of evidence at the trial. Without the use of blockchain, the criminal justice system is more vulnerable to deliberate tampering, without the ability to adequately monitor and record evidence to prevent the probability of unlawful changes.[27]

3.2. *Decentralisation*

Decentralisation increases the redundancy of the data. Compared to current systems that use traditional digital databases, the dispersed character of the blockchain ledger makes it extremely difficult to be compromised, and the possibility of information being tampered with is significantly lessened. The decentralised nature of blockchain guarantees that inherent problems of the system, like hardware and software malfunctions, do not influence the integrity of the data, as it has multiple copies stored on each node of the network, which is further stored in a decentralised cloud system.[28]

3.3. *Transparency*

It has already been argued that blockchain can give birth to an

[27] S. Cheng, M. Daub, A. Domeyer, M. Lundqvist, *Using blockchain to improve data management in the public sector*, 2017<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>.

[28] M.A. Tasnim, A.A. Omar, M.S. Rahman, *Crab: Blockchain-based criminal record management system*, in Proceedings of the 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2018, pp. 294-303.

immutable and transparent chain of custody for evidence. Each change is verified and recorded by the network of nodes, making it almost impossible to alter the records without being detected. The tamper-proof nature of blockchain ensures that the source of the evidence can be traced with complete transparency. Every modification will be recorded on the blockchain as a transaction and is, therefore, clearly visible on the entire network, since data updated by a node has to be verified by multiple of them, falsified data could be spotted and not easily enter the blockchain.[29] Thanks to the transparency offered in the chain of evidence, officers and investigators would not have to respond to an unbearable number of general questions, allowing them to spend their time on further public service. By removing the possibility of tampering with the evidence or criminal records data due to thorough accountability, corruption inside the law enforcement agencies will also be combated more successfully.

The ability to recapture the 'state' of the evidence at each transition point in the chain of custody does not in itself fight tampering, loss, or destruction of the evidence but it improves the likelihood of reporting any suspicious altering activity by the person receiving the evidence, as they would be in the position to compare fast the 'state' of the item when the person who handed it to them originally conceived it with the 'state' in which the item was received by them, allowing them to report any differences or controversies and identify the exact place and time in the chain of custody when the node proceeded with the tampering. It is obvious to all what 'state' the information was at every handling point, who was in charge of it, and how it has evolved since.

This journey creates a path, a map, and a kind of accessible digital trail of the collected evidence to judges, prosecutors, defense attorneys, and investigators. The determination of the validity of the available evidence and the facts of each case turns out to be much easier, increasing the speed of the trial process and decreasing the chances of admitting irrelevant, less viable, or damaged evidence. The outcome, among which could be the dismissal of frivolous cases or the inadmissibility of some evidence, would be determined sooner. If the evidence is ruled inadmissible, it can be disallowed from the court without amending the blockchain or the hash. The same goes for the individual accused, who apart from the legitimate interest, would now also have the capacity to compare the most recent hash against the evidence collected at the beginning of the investigation

[29] T. T. A. Dihn, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, *Untangling blockchain: A data processing view of blockchain systems*., IEEE Data Engineering Bulletin, no. 30(7), 2018, pp. 1366–1385.

to make sure that they have not been victims of any unlawful change or intervention, of intentional tampering, to prevent abuse of their rights and possibly their false convictions.[30] An a priori stipulation of the validity of the evidence, both by the defense and the prosecution, is feasible, allowing a reduction of the number of trials, costs, and time invested in their organisation and realisation.[31]

The key feature of immutability promises that the blockchain, when used in criminal justice procedures, remains intact, accessible to authorised nodes, and protected against any unlawful change that will be detectable. Its decentralised nature diminishes the possibility of any attack and increases its security while guaranteeing interoperability across agencies. Openness and transparency, two further aspects of blockchain, lighten the burden of law enforcement officers and prevent corruption. As any alternation can easily be detected and attributed to a node, the work of the judges turns out much easier. They are in place, even beforehand, to decide upon the admissibility of the collected evidence and to accelerate the trial procedure. The latter leads to a reduction of the costs and the time invested in each case. The ability of the accused or convicted to question the evidence safeguards their interests, their right to a fair trial, and the presumption of innocence. In total, the application of blockchain in the premises of the criminal judicial process could be beneficial for all the parties involved in it, but also for the notion of democracy, fairness, and justice.

4. *Concerns of the use of judicial blockchain*

After explaining all the advantages that the usage of blockchain might bring, it is high time to wonder why it has not been widely applied yet in Europe. The answer might not be so simple. When it comes to technology conflicting with fundamental rights, the EU always appears conservative and hesitant in applying it, prioritising procedural safeguards over speed. Although blockchain might be associated with many positive outcomes in the field of criminal justice, some dark points exist that have raised concerns about its trustworthiness, its security, its ramifications to privacy, and generally its lawful use in procedures by which human rights

[30] Anderes, Baumel, Grer, Veun, Wright, *The use of blockchain within evidence management system,* cit.

[31] Cheng, Daub, Domeyer, Lundqvist, *Using blockchain to improve data management in the public sector*, cit.

and freedoms are deeply affected. These concerns, especially regarding trustworthiness and data integrity, should not be overlooked.

4.1. *Trustworthiness*

Blockchain might be a transparent tool for following the sequence of a criminal investigation and the evidence collected throughout it, but the chance of the latter being falsified cannot be eliminated. Despite its immutability, the data uploaded from the parties ab initio has probably been fabricated, forged, or altered in bad faith. The first input of evidence, especially if uploaded once, cannot be cross-referenced by the rest of the nodes, and, due to that fact, doubts of its trustworthiness may arise. Still, if multiple versions of evidence have been separately uploaded on the blockchain and a dispute arises, it cannot be easily foreseen which one is the original, the one that corresponds to reality and truth, which is the ultimate goal of the judicial procedure.[32]

4.2. *Security*

Blockchain might be tamper-resistant and safer due to its decentralised character in comparison to traditional databases, but that does not mean that it remains unscathed by cyberattacks. While the list of nodes will be exhaustive and the arithmetic database is quite large, its quantity can be exhausted. With the rapid development of computer technology and huge improvements in computational power, there will be a rise in related crimes, allowing quicker, easier, and more effective attacks on hash algorithms, as the ones used in criminal justice blockchains. This prospect coexists with the one of false consensus. In case hackers take control of a significant part of the network computational power, they could manipulate the consensus mechanism, affecting its course and causing errors to the majority opinions and the entire blockchain network.[33]

[32] Internet Law Watch., *The nation's first judicial blockchain: the underlying system of future litigation has been paved*, cit.
[33] *Ibid.*

4.3. *Fundamental Rights*

The most important implications of blockchain that have been the main reason for expressing second thoughts about its application in criminal justice have been those of EU fundamental rights. The right to a fair trial is one of the basic principles of a democratic society. The latter is fulfilled and protected only in case the rights of the suspects, the accused, and the victims are safeguarded. All of them will be most intensively influenced by the involvement of blockchain in criminal justice. Consideration should also be put on another right, the one to privacy and protection of personal data, concerning also the victims and the involved third parties in criminal investigations.

4.3.1. *Right to information*

The aspect of the right to information that is at stake with the use of blockchain is the right to access the materials of the case, meaning the access to the material evidence, whether for or against the suspect or accused person, which is in the possession of the competent authorities about the specific criminal case. The individual should be granted access to materials such as documents, photographs, audio, and video recordings. The latter may be contained in a case file or otherwise held by competent authorities in any appropriate way. Access can be refused where it may lead to a serious threat to life or the fundamental rights of another person, or it is strictly necessary to safeguard an important public interest. Any refusal must be weighed against the rights of the defense of the suspect or accused person, taking into account the different stages of the criminal proceedings, whereas restrictions should be interpreted strictly and in accordance with the right to a fair trial as it is perceived in the European Convention on Human Rights (ECHR) and interpreted by the European Court of Human Rights (ECtHR). There is no obligation for the introduction of new mechanisms or any additional administrative burden. Suspects or accused persons or their legal representatives should have the right to challenge the possible failure or refusal of the competent authorities to provide access. However, member states do not have to cater for the introduction of a specific appeal procedure, a separate mechanism, or a complaint procedure in which such failure or refusal may be challenged.[34]

The deployment of blockchain in the chain of custody and the

[34] European Parliament & Council of the EU. (2012). Directive 2012/13/EU on the right to information in criminal proceedings. OJ L 142, 1.6.2012, pp. 1–10.

distribution of evidence might either make it easier or pose an obstacle to the right to access evidence. If the individuals involved or their lawyers are added as nodes to the blockchain, they could follow the flow of evidence throughout the criminal procedure. Otherwise, digital illiteracy on their part or secrecy and confidentiality of the criminal procedure might leave them outside of it and render them incapable of questioning or challenging the evidence, restraining their right to access evidence and, subsequently, the one to information prescribed in EU Law.

In *Funke v. France*, the ECtHR underscored that compelling a person to produce documents can infringe the right to silence and a fair trial under Article 6(1) and (2) ECHR, a cautionary principle for blockchain-based evidence-sharing systems. In *Al-Khawadja and Tahery and Blokhin v. Russia*, the Court stressed that evidence against the accused must be subject to adversarial challenge, a requirement that blockchain interfaces must facilitate. Otherwise, risk procedural unfairness.

4.3.2. *Presumption of innocence*

A vital aspect of the presumption of innocence constitutes the right of suspects and accused persons to be present at the trial. Although it is not an absolute one, as, under certain conditions, it can be waived, it might be provoked by the possible automation of the adjudication process promised by the technological domination of blockchain. It should, thus, be noted that the right to be present at the trial can be exercised only if one or more hearings are held, meaning that the right to be present at the trial cannot apply if the procedure does not provide for a hearing, which might occur if a case is dismissed at an earlier stage.[35]

If adjudication is partially automated, safeguards are required to preserve core fairness guarantees. In C-688/18 (*TX and UW*), the Court of justice of the EU (CJEU) held that trials in absentia can only comply with the presumption of innocence when the accused is notified in time, represented, and given a real opportunity to participate or have evidence reheard. Therefore, any blockchain-supported adjudication must preserve these procedural safeguards.

4.3.3. *Right to privacy and protection of personal data*

The challenges posed by the relationship between blockchain

[35] European Parliament & Council of the EU. (2016). Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.

technologies and the implementation of the General Data Protection Regulation (GDPR)[36] and relevant legislation[37] reveals a possible clash between the protection of privacy, on the one hand, and the promotion of innovation, on the other hand. Since judicial blockchain contains personal data, its immutable nature is likely incompatible with the right to erasure set out in Article 17 of the GDPR. In the blockchain environment, evidence and data cannot be erased at the request of the data subject.[38] While full deletion of data is difficult, approaches such as off-chain data storage combined with encryption key destruction may provide compliant alternatives.[39]

Other rights, also, can be problematic in a blockchain context too, including the right to the rectification of personal data.[40] Such rectification or erasure of personal data should be communicated to recipients to whom the data has been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data, which is more challenging in the case of blockchain technologies.

Data in the form of evidence is stored in a chain of blocks in several locations. As long as each block has access to its predecessor, all other data can be stored in a decentralised manner.[41] As a result, in despised blockchains such as the judicial one, it can be difficult to identify data controllers and processors as defined under GDPR, and, hence, enforce their obligations, bringing up issues of jurisdiction and access points. Particularly in cases where it is difficult, or perhaps impossible, to identify a data controller, it

[36] European Parliament & Council of the EU. (2016c). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88.

[37] European Parliament & Council of the EU. (2016). Directive (EU) 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. OJ L 119, 4.5.2016, pp. 89–131.

[38] European Union Blockchain Observatory, *Blockchain and the GDPR*, n.d., <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf>., pp. 5.

[39] CNIL, *Blockchain et RGPD: Quelles solutions pour un usage responsable en présence de données personnelles?, 2018,* <https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles>.

[40] European Union Blockchain Observatory, *Blockchain and the GDPR*, cit.

[41] European Commission, *Shaping Europe's digital future: Blockchain and Web3 strategy,* n.d. <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>.

can naturally be tricky to enforce the GDPR's requirements for the data controller. This ambiguity surrounding data controllership in blockchain systems, flagged by Finck and Pallas,[42] undermines compliance with the GDPR's accountability principle (Art. 5(2)).

Moreover, the proliferation of copies of data in a blockchain is likely incompatible with the data minimisation principle set out in Article 5 of the GDPR.[43] In *S. & Marper v. UK*, retaining biometric data after acquittal was deemed a violation of Article 8 of the ECHR due to its disproportionate interference. At this point, a parallel could be drawn to concerns about immutable data stored on-chain against its indefinite storage post-proceeding.

Much debate has arisen around the anonymisation of personal data to comply with the relatively high standards set by the GDPR. The hashing of data cannot be considered to be an anonymisation technique in many circumstances. In *Breyer v. Germany* (C582/14), the CJEU clarified that even pseudonymised data can constitute personal data if re-identification is possible. Consequently, any blockchain system that logs judicial outcomes, especially when those include names, timestamps, or hashed identifiers, must either irreversibly anonymise the data or restrict access in compliance with GDPR principles. Similarly, in *WM and Sovim SA v Luxembourg Business Registers* (C37/20), the Court stressed that transparency must be balanced against fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU. This implies that judicial blockchain applications must limit data visibility to actors with a legitimate legal interest, most feasibly through a permissioned architecture.

For criminal justice blockchain, those worries would be smoothed by launching a private, permissioned blockchain network, which is designed in a way that every piece of data is readable by only the competent nodes, by the parties that need to, namely, the agencies involved in the criminal investigation. Still, the ECtHR's ruling in *Podchasov v. Russia* reaffirmed that strong encryption and the protection of digital communications are integral to Article 8 ECHR. This judgement underscores the need for blockchain-based judicial tools to maintain confidentiality and resist any form of surveillance or unjustified data exposure.

[42] M. Finck, S. Pallas, *Trust in Blockchain Technology and the Digital Transformation of the Public Sector*, in European Journal of Risk Regulation, no 11, 2020, pp. 712.

[43] European Parliament. (2018). Resolution on blockchain: A forward-looking trade policy (2018/2085(INI)). Strasbourg, December 13.

4.4. *Possible Solutions*

Regardless of the alarming aspects of blockchain, there are, unarguably, still some ways to combat efficiently those challenges, starting with raising awareness, educating, and enhancing technical expertise on blockchain. As long as this technology is relatively novel, most people are either completely ignorant or lack an understanding of its basic features and characteristics. But this is not limited to the general population and rather concerns the experts involved in the proceedings and the administration of criminal justice. The absence of clear guidance and the uncertainty regarding how the technology can be applied within the legal framework, as there is limited case law and almost no precedent around it, has led to a conservative and resistant view towards blockchain on behalf of the judicial community.[44] A first step would be through information campaigns, training, and the adoption of an EU regulatory framework foreseeing common standards for the application of blockchain to criminal justice, possibly based on existing blockchain guidelines. This would help overcome differences between the rules applied in the member states and could enhance the conduct of criminal investigations throughout the EU, bringing judicial cooperation even closer.

Constant conduct of research in the field, with the involvement of ethicists, jurists, investigators, and policymakers, would create a multidisciplinary scientific environment, where all sides could be represented, both at the stage of development and at that of deployment. This initiative should be conducted on an EU level, where all the member states would be engaged in an exchange of good practices, technical and scientific expertise, views, and social, political, legal, or ethical concerns so that all voices, even the more skeptical or conservative ones, are heard. Technology developed on consensual legal and ethical standards would be more trustworthy, and advanced in matters of security and its incorporation in the criminal justice system and, therefore, widely acceptable.

As far as human rights implications are concerned, conducting a pre-emptive review of issues surrounding the infringement of rights and abuse that may arise would offer an answer to the questions raised before.[45] An

[44] ND, *How can blockchain technology be applied to chain of custody,* in Chain Research, 2019, <https://www.chain.com/blog/how-can-blockchain-technology-be-applied-to-chain-of-custody>.

[45] J. Yun, H. Chun, J. Kim, B. Ryu, W. Lee, B. Lee, M. Kim, *The criminal justice response and development strategy in the age of the Fourth Industrial Revolution (II): The Internet of Things (IoT) and blockchain*, in Trends & Policies in Criminal Justice, Korean

evaluation of the relevance of using blockchain instead of any other type of secure and encrypted communication channel should proceed, followed by human rights impact assessments, which should be drafted in cases of employment of blockchain to criminal procedure to ensure that the latter fully conforms with the EU data protection framework and fully respects the principles set out in EU law, particularly concerning the rightful processing of personal data. At this point needs of vulnerable persons should also be taken into account. If adequately designed, blockchain technology should be in line with the principle of 'data protection by design', which serves to give data subjects more control over their data, in line with the GDPR, when this is also feasible and compatible with their rights and the demands of the criminal investigation and judicial proceedings. The participation in the discussions by issuing guidelines and recommendations of EU institutions, such as the European Data Protection Board, would be crucial to ensure that blockchain technology is compliant with EU law. Law enforcement agencies and the judiciary should be in a position to guarantee the compliance of the blockchain system with human rights before it is fully utilised under their auspices, fulfilling the demand for 'data protection by default'.[46]

5. *Conclusions*

Blockchain is identified as blocks of data connected in a decentralised system, mainly used for transactions. This technology has, in the last decade, entered the legal sphere. The EU has expressed its willingness to adapt emerging technologies for the improvement of cross-border judicial cooperation and administration of justice, as long as the need for quick, effective, and reduced-cost resolution of a criminal case has become the priority of law enforcement agencies and the judiciary. Unlike the US and China, the counter-technological power is already using a national judicial platform for blockchain evidence, connecting the blockchains of several local courts in China and incorporating a chain of credible evidence generated by them based on blockchain technology. In the investigative field, blockchain is also present. Most notably, the tracking results by surveillance parole of offenders by law enforcement in a Chinese region are

Institute of Criminology, no. 013, 2021.

[46] European Union Blockchain Observatory, *Blockchain and the GDPR*, cit.

produced with blockchain technology.

With the blockchain technology trend, the potential of its use cases for criminal justice purposes has entered the policymakers' agendas. Among those purposes, the most eminent one is the utilisation of blockchain for warrants, issued by courts or prosecutors, and further modified by the investigators. Such an action would enable the latter to constantly update the blockchain record with the actions they took and the evolution of the charges throughout the judicial process, making it easier to follow the criminal investigation, to control the involvement of each factor, and to verify its accordance with the law. Moreover, the dramatic increase in digital evidence has a great impact on criminal investigations. Since digital evidence is vulnerable, maintaining its integrity and authenticity has been a crucial task.[47] Blockchain can fulfil this task successfully by offering a tamper-resistant way of documenting and sharing the chain of custody, evidence, and assets, allowing a significant reduction of its loss, theft, and mishandling. Since, for the time being, the scenario of blockchain-based dispute resolution is far-fetched, its usage for the update of judicial decisions, so as for them to reflect the most current circumstances, is compatible with the right to fair trial and the presumption of innocence. The same could be argued for the introduction of blockchain to criminal records for their secure modification and distribution before and after a criminal trial.

Those use cases of blockchain for criminal justice are expected to benefit the latter largely. First of all, they would enhance the immutability of custodial chain, evidence, and official documents such as warrants, verdicts, and records produced and kept throughout adjudication, since nobody would be able to alter anything secretly but only the nodes with granted access that can be traced are in the position to add and remove information. This situation guarantees the integrity and accountability of the data, which cannot be affected by any external problems as software or hardware issues, due to the decentralisation feature of the blockchain. A violation is, simultaneously, more difficult, as the transparent nature of blockchain creates an open flow of information distributed by diverse factors at different stages of the criminal process. Each step of the procedure, as well as any unlawful alteration, can be traced, making it harder for the corruption of the judiciary or law enforcement and facilitating interoperability between the agencies. The court would, therefore, be

[47] Tsai, *The application of blockchain of custody in criminal investigation process,* cit., pp. 2780.

capable of deciding upon the admissibility of the evidence beforehand, and the accused individual could question the collected evidence, safeguarding fairness in judicial procedures, democracy, and justice.

Despite the benefits, some concerns have been expressed regarding the introduction of blockchain to criminal procedure. To begin with, questions have been raised about its trustworthiness and security. Although in general terms it is a reliable technology, the chance of its content being falsified or attacked cannot completely vanish. Technology is always advancing but yet it has not reached the level of complete immutability and invulnerability. The most serious drawback of blockchain has been its interference with fundamental rights as prescribed in the EU legislation, with a focus on the right to privacy and protection of personal data. As confidentiality is a strict prerequisite of criminal justice procedures given the presumption of innocence, right to defense, an effective remedy, and a fair trial, the ramifications of a variety of architectural decisions, such as the openness of networks, public access to them or the readability of the stored data should be addressed before its application.

Those concerns do not mean that the application of blockchain is doomed. They should be regarded as challenges, upon which the EU community should answer before enacting its vision of blockchain integration into criminal justice.

To fully align blockchain-based innovations with the EU's constitutional and legal commitments, any future framework should incorporate several normative safeguards. First, a sector-specific legislative instrument for blockchain in justice could be adopted, clarifying the roles and responsibilities of nodes as either data controllers or processors under the GDPR. Second, the development and deployment of blockchain systems should be preceded by ex ante human rights and rule-of-law impact assessments, ensuring compliance with Article 52(1) of the Charter of Fundamental Rights. Third, judicial oversight mechanisms must be embedded into blockchain infrastructures, for instance, through time-stamped logging of access by identifiable judicial actors and adversarial contestation features for defendants. Fourth, technical standards should be co-developed by legal and cryptographic experts, adopting a rights-by-design model similar to privacy by design under the GDPR. Finally, institutional coordination through an EU-level oversight body, potentially under the remit of the European Data Protection Supervisor or the Fundamental Rights Agency, could ensure harmonisation and accountability. These normative recommendations are consistent with the precautionary principle in law and with emerging

scholarship that views blockchain not merely as infrastructure but as law-relevant code that must be subjected to democratic and legal scrutiny.

Training of the judicial and investigative staff, awareness-raising campaigns of the public, and the drafting of a strong, comprehensive, and commonly agreed-upon legal framework constitute viable solutions. Along with them, further research with the goal of constant improvement of blockchain technologies has been suggested. It should also be ensured that electronic evidence is recognised and is admissible by the legal and judicial systems of the EU member states. Otherwise, blockchain technologies will remain an impractical tool within the EU sphere.

Rather than overregulating or rejecting new technologies as inherently harmful, policymakers should adopt a balanced, evidence-based approach that addresses both potential risks and opportunities. Keeping 'human in the loop' in the regulatory framework and guaranteeing that by design and by default all kinds of technologies are deployed to satisfy human needs and transparent, fair, trustworthy, secure, and in accordance with fundamental rights, principles, and standards distribution of justice inside the EU is the biggest challenge law and policymakers, law enforcement agencies, technical experts and the judiciary will face shortly. Balancing is achievable if all the involved factors have as a starting point and as a compass the amelioration of their position, the accused or suspects' position, and the judicial system as a whole towards a democratic, fair, technologically advanced, and humanistic one.

Andreas Kanakakis*

Introducing Digital Investigative Measures in Criminal Proceedings: 'The Double-Edged Sword' **

1. *Introduction*

The advancement of new technologies has profoundly affected nearly every aspect of life, including the way crime is committed, investigated and prosecuted. Cybercrime has become a broad and evolving concept, referring to all "criminal acts using electronic communications networks and information systems or against such networks and systems",[1] encompassing not only crimes unique to the digital world, such as attacks against information technology (IT) systems, but also conventional forms of crime, such as fraud, forgery or harassment.[2] Such crimes can now be

* PhD Candidate at University of Luxembourg & Vrije Universiteit Brussel.

** Acknowledgement: This article is written within the framework of the PROMODE project, supported by the Research Foundation – Flanders (FWOAL1089) and the Luxembourg National Research Fund (INTER/FWO/22/17204313).

[1] For the definition of cybercrime, see the Communication of 22 May 2007 from the European Commission to the European Parliament, the Council and the Committee of the Regions, 'Towards a General Policy on the Fight against Cybercrime', COM(2007)267 final, 2.

[2] See J.J. Oerlemans, *Investigating cybercrime* (Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University 2017) 20, who makes a distinction between target cybercrimes, i.e. crimes in which a computer is the target of the offence, and tool cybercrimes, where a computer is used to facilitate the commission of a traditional crime.

committed remotely and on a large scale, challenging the investigation capabilities of law enforcement authorities.[3]

Especially in times when people are more and more interacting in virtual environments, criminal activity has surged in digital spaces,[4] with perpetrators taking advantage of advanced techniques to obscure their identity and protect their communications. To achieve anonymity, cybercriminals frequently access the Internet through various networks or use anonymisation tools such as proxy servers, virtual private network (VPN) services or anonymity networks (e.g. Tor or Freenet),[5] which make it harder for law enforcement agencies to trace their IP addresses and digital footprints. And even when anonymity is pierced, law enforcement authorities often have to overcome the hurdles of encryption, as it is impossible for them to reach the context of the plain text, unless they have the decryption key.[6]

The landscape of cyber-criminality becomes even more complex as it is not familiar to geographical and jurisdictional limits. After facing the challenges of anonymity and encryption, law enforcement operations might significantly be hindered by conflicts of territoriality and jurisdiction. Adhering to the principle of territorial jurisdiction, crime prosecution, as a form of exercising a State's sovereignty, cannot extend outside this State's limits, unless it is explicitly permitted by means of an international treaty.[7] In this context, mutual legal assistance (MLA) frameworks,[8] and mechanisms for crime prosecution and evidence acquisition at European

[3] Communication, (n 1), 2.

[4] See, Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, <www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>; INTERPOL report of August 2020 titled 'Cybercrime Covid-19 Impact', <www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

[5] More at United Nations Office on Drugs and Crime (UNODC) Teaching Module 5: Cybercrime Investigation, <sherloc.unodc.org/cld/en/education/tertiary/cybercrime-/module-5/key-issues/obstacles-to-cybercrime-investigations.html>; J.J. Oerlemans, (n 2), 37-44.

[6] More on encryption, see Oerlemans, (n 2), who distinguishes between encryption in transit and encryption in storage, 44-52.

[7] See J. Kleijssen and P. Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', *Netherlands Yearbook of International Law* (T.M.C. Asser Press 2016), 147-173.

[8] For example, see Agreement of 19.7.2003 on mutual legal assistance between the European Union and the United States of America, <eur-lex.europa.eu/eli/agree_internation/2003/516(2)/oj/eng>.

Union (EU) level,[9] become relevant, facilitating cross-border cooperation of law enforcement authorities in their fight against cybercrime.

To meet the growing demands of criminal investigations, law enforcement powers are also considerably strengthened, as they encompass a wide array of practices, ranging from collecting publicly available online information and online undercover investigations to the issuance of data production or preservation orders to online service providers and the utilisation of cutting-edge tools such as hacking or Artificial Intelligence (AI). For the purposes of this study, the focus is placed on three groups of methods, which facilitate access to and processing of data with minimum human intervention, namely, collecting publicly available online information, performing police hacking, and utilising AI tools.

However, the introduction of digital investigative measures into the arsenal of law enforcement practices has significantly outpaced regulation, both at national and EU levels. Their remote and covert application alongside jurisdictional particularities present new challenges that necessitate a reconceptualisation of traditional limitations regarding the conduct of criminal investigations and, subsequently, a re-evaluation of national criminal procedural rules governing the conduct of investigative measures. In the end, the debate moves to the core of fundamental rights and their alignment with the way digital investigative measures are executed, raising the key question: In whose favour must the scale tip when utilising digital investigative measures – law enforcement or the individual?

This paper will embark on a short, non-exhaustive exploration of certain digital investigative measures, address complexities of their application and conclude by examining concerns surrounding their interaction with the fundamental rights of the affected person.

2. *Digital Investigative Measures: Three Examples*

2.1. *Collecting Publicly Available Online Information*

The interaction of individuals in online environments provides law

[9] See in particular, Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA), and Directive of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (2014/41/EU).

enforcement with a valuable tool. Publicly available online information –often referred to as Open Source Intelligence (OSINT)– includes data from open sources such as web applications, social media, satellite images, and more.[10] This information is accessible to all Internet users, making it an attractive resource to the police.[11] Although acquiring this data may seem to require the least possible effort for law enforcement (especially when performed automatically), privacy concerns may also arise, challenging the lawfulness of the measure.[12]

For the collection of publicly available online information two main methods can be applied: (1) manual, and (2) automatic searches. The first one entails law enforcement officers entering keywords linked to the person under investigation into a search engine (e.g. Google) in order to derive relevant information from the content concerning that person, without storing the results of the search.[13] In contrast, using automated systems, able to parse through and process large amounts of data, entails compiling data from pertinent online sources on a regular basis and storing it in ways that guarantee timely access to relevant information.[14]

An advanced method for OSINT collection can be found in the use of web crawlers, commonly referred to as bots or spiders,[15] whose application for evidence collection purposes is considerably expanding. Web crawlers have the capacity to methodically scan web pages, link them to one another and collect, analyse, and store information (usually URLs) within the

[10] D. Quick and K.K. Raymond Choo, 'Digital Forensic Intelligence: Data Subsets and Open Source Intelligence (DFINT+OSINT): A Timely and Cohesive Mix' (2018) 78 *Future Generation Computer Systems* 558, 560, <www.sciencedirect.com/science/article/pii/S0167739X16308639>.

[11] In fact, intelligence-led policing is no longer limited to crime prevention, but acquires a repressive approach, being used for evidence collection and crime investigation and prosecution, *ibid.*

[12] B.J. Koops, 'Police investigations in Internet open sources: procedural-law issues', 29 *Computer Law & Security Review* (2013) 655, <www.sciencedirect.com/science/article/pii/-S0267364913001660>, who aptly argues that, despite sharing data with everyone, individuals do not expect their data to be literally subject to everyone's scrutiny, while its collection by law enforcement officials goes a mile further, especially when it becomes systematic or is combined with data storage in police databases.

[13] *Ibid.*, 656.

[14] Q. Eijkman and D. Weggemans, 'Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability?', (2012) 23 *Security and Human Rights* 4, 285-296.

[15] Z. Gold and M. Latonero, 'Robots Welcome? Ethical and Legal Considerations for Web Crawling and Scraping', (2018) 13 *Washington Journal of Law, Technology and Arts* 3, 280-282, <digitalcommons.law.uw.edu/wjlta/vol13/iss3/4/>.

context of a specific search.[16] While this ability was traditionally limited to text and basic website metadata, advancements in technology now allow the collection of more complex datasets, including images, user comments or personal identifiers.[17]

The use of web crawlers may be determined by their operators, but most commonly it is algorithms that direct their searches and operations. Especially with the rise of AI, it is now possible for a crawler to automatically visit certain websites many times per day to ensure that the data collected is updated or complemented by new information.[18] As the particular tool deploys AI to scan large databases of data and link it to specific persons, without concrete rules on its use and judicial oversight guarantees, the possibility of crossing the line between legitimate evidence collection and excessive interference with the rights to privacy and data protection seems higher. After all, it is not only the search itself but also the following processing and sometimes retention of data by law enforcement agencies (LEAs).[19]

2.2. *Hacking As an Investigative Tool*

Hacking can become an increasingly prominent method in criminal investigations, enabling law enforcement agencies to gain access to computer systems for various purposes, among which are surveillance and evidence collection. Infiltrating an IT system,[20] in order to manipulate it

[16] M. Javed, 'How do Internet Search Engines Work?', 2004 Scientific American, www.scientificamerican.com/article/how-do-internet-search-en/.

[17] Gold and Latonero (n 15), also citing 'What are Crawlers? How do they work?', SEO marketing world, <www.seomarketing-world.com/seo-faq/crawlers.php>.

[18] With regard to facial recognition tools, L.M. Landerer, 'Things that are Different Are Not the Same: Die automatisierte Analyse massenhafter Internetdaten und die Vorratsdatenspeicherung' (2024) *Verfassungsblog*, <verfassungsblog.-de/things-that-are-different-are-not-the-same/>, aptly illustrates the example of PimEyes, alongside its challenges regarding the balance between privacy and the need for efficient law enforcement.

[19] *Ibid.*, contrary to C. Thönnes, 'Daniela Klette und die Frucht der vergifteten Maschine' (2024) *Verfassungsblog*, <verfassungsblog.de/klette-und-die-frucht-der-vergifteten-maschine/>.

[20] The Council of Europe's Convention on Cybercrime uses the term 'computer system' instead of IT system, defining it as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data", Article (1) a. of Council of Europe, Convention on Cybercrime, 23 November 2001, ETS 185.

without the permission of its original user, has become key technique of LEAs against the challenges of anonymity and encryption, enabling them even to 'bypass' security barriers set by the users.[21]

Firstly, hacking can be applied in the form of network searches, which entail law enforcement agents already having a seized device in their possession. Typically, this can take place during a house search where the suspect is aware of the search itself, though not necessarily of the possibility and extent of its expansion to include IT systems and thereto connected devices.[22] In some cases, law enforcement agents may also acquire user credentials and login information so that they gain access to the individual's cloud account and profiles in online platforms.[23]

Secondly, searches can take place remotely, in absolute secrecy and involve a more invasive approach. Most commonly without the individual's knowledge, law enforcement agencies can access a computer system, retrieve and copy stored data,[24] or take screenshots, all while circumventing encryption and anonymisation techniques.[25] Remote access to an IT system may prove particularly useful in cases where law enforcement needs to identify suspects via their IP address or prevent data from being encrypted, before it becomes accessible.[26]

Security features can furthermore be circumvented by exploiting vulnerabilities of the IT system and installing monitoring software.[27]

[21] O. Kerr, 'Norms of Computer Trespass' (2016) 116 Columbia Law Review 143, p. 11164; R. Clifford, Cybercrime – The Investigation, Prosecution and Defense of a Computer-Related Crime (Carolina Academic Press 2011), 94; See also, S. Bellovin et al, 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet' (2014) 12 *Northwestern Journal of Technology and Intellectual Property* 1, 1-64.

[22] C. Conings and J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?' (2013) 5 *Computerrecht*, 23-32, <www.recht.nl/-vakliteratuur/ict/artikel/342488/van-een-netwerkzoeking-naar-online-doorzoeking-grenzeloos-of-grensverleggend/>, use the example of LEAs seizing a computer during a house search and proceeding to access connected devices such as external hard drives or media players, actively broadening the search beyond the physical space.

[23] *Ibid.*; J.J. Oerlemans and M. Galič, 'Cybercrime investigations', in W Van der Wagen, J.J. Oerlemans and M. Weulen Kranenbarg (eds), *Essentials in cybercrime: A criminological overview for education and practice*, (Eleven Publishers / Boom Juridische Uitgevers 2021), 197-254.

[24] S. Brenner, 'Dissonance, and Remote Computer Searches' (2012), 14 *North Carolina Journal of Law and Technology* 1, 43-92, <scholarship.law.unc.edu/ncjolt/vol14/iss1/4/>.

[25] Oerlemans and Galič, (n 23), 220 ff.

[26] Oerlemans (n. 2), 54.

[27] See B. Jacobs, 'Policeware' (2012) 39 *Nederlands Juristenblad*, 2761, www.recht.nl/vakliteratuur/alletijdschriften/aflevering/19709/nederlands-juristenblad/2012/39/, who

Weaknesses of the target IT system can be manipulated through various types of malware, including viruses, worms and trojan horses.[28] The installation of such software obviously happens without the targeted person's knowledge, however, in most cases, the target's cooperation is necessary. To this end, law enforcement agents usually trick targets into opening monitoring software in the form of email attachments or meeting access links, thereby unknowingly cooperating in the installation of that software in their computer systems.[29] After successful installation, policeware secretly obtains control of a system's functionalities for the purposes of the criminal investigation. LEAs can activate a computer's built-in microphone or intercept its keystrokes, or even create 'backdoors' to the system, which enable direct access to and observation of the targeted person's activities in real time.[30]

In legal context, hacking as the unauthorised access to IT systems and exploitation of their vulnerabilities consists a highly intrusive technique, which beyond law enforcement context is considered an illegal act.[31] Given the potential for abuse,[32] hacking as an investigative tool necessitates careful regulation, with particular emphasis on judicial oversight (e.g. the issuance of a warrant before its application).[33]

uses the term "policeware" to define computer monitoring software installed for these purposes.

[28] For the definitions of each type of malware, see 'What is malware? Prevention, detection and how attacks work',www.techtarget.com/searchsecurity/definition/malware.

[29] See the example of trojan horses being installed during airport checks examined by Andreas Kraft, 'Trojaner am Flughafen aufgespielt' (2019), *Frankfurter Rundschau*, <www.fr.de/politik/trojaner-flughafen-aufgespielt-11696257.html>.

[30] M. Pisarić, 'The Use of Policeware to Hack Electronic Evidence in Germany and the Netherlands' (2023), 28 *NBP Journal* 1, 16-26.

[31] See Explanatory Report of Cybercrime Convention of 23.11.2001 – ETS 185, para 44, where it is explicitly noted that "'Illegal access' covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself […]."

[32] See, G. Wilde and E. Landi, 'Exploring Law Enforcement Hacking as a Tool Against Transnational Cyber Crime' (2024) Carnegie Endowment for International Peace, <carnegieendowment.org/research/2024/04/exploring-law-enforcement-hacking-as-a-tool-against-transnational-cyber-crime?lang=en>.

[33] On the *ex ante* or *ex post* judicial control, see for instance ECtHR, judgment of 04.12.2015, *Roman Zakharov v. Russia*, App. no. 47143/06, esp. para 233; ECtHR, judgment of 06.09.1978, *Klass and Others v. Germany*, App. no. 5029/71, para

2.3. *The Use of Artificial Intelligence*

Artificial Intelligence tools are gradually making their way into the game of law enforcement as they offer unparalleled possibilities, from the assessment of already collected evidence to the generation of new leads and the completion of incomplete data.

In the field of data analytics, large language models (LLMs) and Natural Language Processing (NLP) capabilities are used to facilitate the processing of voluminous text-data to extract critical insights, detect patterns, and signal suspicious activity. LLMs may also be used to enhance efficiency through automated summarisation, object recognition, and geo-spatial analysis, though human review remains essential to ensure accuracy.[34] Text summarisation, classification, clustering and machine translation are further supported by NLP techniques, which assist in threat identification and the extraction of actionable information from unstructured text.[35]

AI uses extend to digital forensics, offering tools that specialise in extracting, processing, and analysing digital evidence from seized devices and data sources. [36] Such tools are capable of identifying file types, parsing through structured or unstructured data, reconstructing fragmented files, and establishing connections between traces, data, activities.[37] In the realm of visual monitoring and image classification,[38] AI tools enable the early detection of suspicious activities and the identification of persons of interest through facial recognition or other biometric identifiers.[39] Last but not

55; CJEU, judgment of 06.10.2020, *La Quadrature du Net and Others*, joint cases, C-511/18, C-512/18, C-520/18, para 189.

[34] G. Roebling and B. Necula 'Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud' (2024) 3 *eucrim* 206, 207-8.

[35] Europol Innovation Lab, Observatory Report of 10 September 2024, "AI and policing: The benefits and challenges of artificial intelligence for law enforcement", 12, <www.europol.europa.eu/publication-events/main-reports/ai-and-policing>.

[36] For example, Hansken is a commercial tool deployed by Dutch law enforcement agencies for these purposes. See more at <www.hansken.nl>.

[37] H.M.A. Van Beek et al, 'Digital Forensics as a Service: Stepping up the Game' (2020) 35 *Forensic Science International: Digital Investigation* 301021, 4.

[38] See Europol Innovation Lab, Observatory Report, (n 35), 22-3, suggesting that the use of AI algorithms for image categorisation may guarantee the accuracy and efficiency of criminal investigation, as it makes sure that every important piece of visual evidence is accurately categorised as 'suspicious' or 'non-suspicious' or according to its theme, date, time etc.

[39] A relevant example comes from the algorithmic video-surveillance for the Olympic Games 2024 in Paris, see 'Sécurité des Jeux Olympiques : «des opérateurs de caméras

least, Generative AI technologies can assist in creating new synthetic data based on patterns from existing content. This capability allows for the generation of various types of media, such as text and images, which are available even when the original data cannot be used in criminal investigations.[40]

One can easily guess that the integration of such technologies in law enforcement settings is accompanied by many challenges. Opacity of AI tools, especially those employing complex algorithms, raises important issues. The inability to understand how certain AI models arrive at their outputs, also referred to as 'black-box',[41] makes it difficult for law enforcement officials, judges and defendants to assess the validity of those systems and the accuracy and reliability of their output.[42] The lack of transparency is particularly concerning in high-risk systems,[43] whose output may have a profound impact on an individual's life.[44] If the way the system operates is obsure, so is the decision stemming therefrom, making accountability difficult to address and significantly undermining the rights of the person concerned.

augmentés»' 07.08.2024, <www.interieur.gouv.fr/actualites/actualites-du-ministere/securite-des-jeux-olympiques-des-operateurs-de-cameras-augmentes>; 'JO 2024 : de la vidéosurveillance algorithmique à la reconnaissance faciale, il n'y a qu'un pas' 26.04.2024, available at the official website of Amnesty International France, <www.amnesty.fr/liberte-d-expression/actualites/jo-paris-de-la-videosurveillance-algorithmique-a-la-reconnaissance-faciale-il-n-y-a-qu-un-pas>. For a detailed analysis, see Y. Bouadi, 'Paris 2024 : l'expérimentation de la vidéosurveillance algorithmique à la lumière du règlement européen sur l'intelligence artificielle' (2025), 686 *Revue de l'Union européenne*, 133.

[40] Europol Innovation Lab, Observatory Report, (n 35), 29 ff.

[41] K. Quezada-Tavarez et al, 'Legal challenges in bringing AI evidence to the criminal courtroom' (2021) 12 New Journal of European Criminal Law, 531.

[42] *Ibid.*; J. Burrel, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016), 3(1) *Big Data and Society* , <journals.sagepub.com/doi/10.1177/2053951715622512>.

[43] Under the classification made in Article 6(2) and Annex III of the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[44] However, see R. Stoykova et al, 'The AI act in a Law Enforcement Context: The Case of Automatic Speech Recognition for Transcribing Investigative Interviews' (2024), *SSRN*, <ssrn.com/abstract=4913090>, who note that even low-risk applications, that offer a significant gain in time and focus, such as Automated Speech Recognition (ASR) systems, capable of converting human speech into text, applied for the transcription of investigative interviews, should also be subject to a 'code of conduct' based on the obligations attributed to developers and deployers of high-risk AI systems.

Another critical challenge is bias and discrimination embedded in AI systems. Models are often trained on historical data that might contain societal biases, reflecting past prejudices and discriminatory practices. As noted in Europol's Observatory Report, if an AI system is trained on data from over-policed communities, it may erroneously suggest that these areas are more prone to crime, reinforcing existing inequalities.[45] Besides, representational bias may add another layer of complexity, as over- or under-representation of certain groups in the datasets used to train AI models may lead to outputs that disproportionately affect those groups.[46]

3. *Challenges in the Introduction of Digital Investigative Measures*

3.1. *Pro-active Surveillance vs. Re-active Investigation*

The increasing convergence of technology and law enforcement has admittedly blurred the lines between crime prevention and crime prosecution,[47] particularly when it comes to surveillance and the use of mass data.[48] As already shown, technological capabilities have provided unprecedented access to electronic communications and data, which can also be leveraged to assess risks and pre-empt criminal activities. Information can be gathered not only at the stage of criminal investigations for crime detection and prosecution, but also through surveillance mechanisms destined to prevent criminal activities. In this context, a key challenge for contemporary criminal proceedings is to prevent surveillance-derived data and potential evidence from bypassing established procedural safeguards in the criminal justice system.[49]

[45] Europol Innovation Lab, Observatory Report, (n 35), 7-8.

[46] European Agency for Fundamental Rights (FRA), Bias in algorithms - Artificial intelligence and discrimination, Report of 8 December 2022, fra.europa.eu/en/publication-/2022/bias-algorithm; G. Malgieri and G. Comandé, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation"(2014) 7(4) *International Data Privacy Law*, 248.

[47] See, ECtHR, judgments of 13 September 2018 (Chamber) and 25 May 2021 (Grand Chamber), *Big Brother Watch and others v the United Kingdom*, Appl. nos. 58170/13, 62322/14 and 24960/15.

[48] See concretely, M. Andrejevic, 'Surveillance in the Big Data Era' in K. Pimple (ed), *Emerging Pervasive Information and Communication Technologies (PICT)* (Springer 2014), 55-69.

[49] See, L. Bachmaier Winter, 'Criminal Investigation, Technological Development, and

The prominent role of intelligence services in law enforcement operations is particularly evident with regard to the fight against terrorism,[50] organised crime and cybercrime.[51] Intelligence agencies are empowered with the technology and expertise to access vast amounts of data efficiently, a capability which enables a more comprehensive threat analysis and the early detection of criminal activities. Without the intelligence obtained for these preventive purposes, law enforcement operations would be significantly slowed down, especially for such complex crimes.

However, this interaction of surveillance and law enforcement comes with its own set of challenges. Unlike criminal investigations, digital mass surveillance often targets unknown individuals, entailing infringements on their rights without any concrete suspicion linked to a specific crime. It comes thus as no surprise that proportionality assessments may differ significantly from those performed in regressive criminal investigations.[52] Indeed, mass surveillance for national security purposes may serve legitimate aims and be necessary in a democratic society, but it must be accompanied by robust regulatory oversight to ensure that it remains proportionate and compliant with human rights safeguards.[53] Even so, national authorities are afforded a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security.[54]

In summary, the distinction between pro-active mass surveillance and re-active criminal digital investigations hinges on two factors: the

Digital Tools: Where Are We Heading?', in L. Bachmaier Winter and S. Ruggeri (eds) *Investigating and Preventing Crime in the Digital Era* (Springer 2022), 3-17.

[50] Concretely about terrorism, see the report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights of the International Commission of Jurists titled 'Assessing Damage, Urging Action' (2009), 67, <www.icj.org/wp-content/uploads/2012/04/Report-on-Terrorism-Counter-terrorism-and-Human-Rights-Eminent-Jurists-Panel-on-Terrorism-series-2009.pdf>; M. Zöller, 'Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung" des internationalen Terrorismus' (2007) *Juristen Zeitung* 15/16, 763-771.

[51] More on the cooperation of German intelligence services and law enforcement authorities, see, M. Zöller, 'Die Zusammenarbeit der Nachrichtendienste mit den Strafverfolgungsbehörden', in J.H. Dietrich et al (eds), Nachrichtendienste in vernetzten Sicherheitsarchitektur (Mohr Siebeck 2020).

[52] ECtHR, judgment of 29 June 2009, *Weber and Saravia v. Germany*, Appl. no. 54934/00, para 106; ECtHR, judgment of 25 May 2021 (GC), *Big Brother Watch and others v. the United Kingdom*, Appl. nos. 58170/13, 62322/14 and 24960/15, para 338.

[53] ECtHR, *Weber and Saravia*, (n 52), para 115; ECtHR, judgment of 19 June 2018, *Centrum för Rättvisa v. Sweden*, Appl. no. 35252/08, para 133.

[54] ECtHR, judgment of 4.9.2013 (Chamber), *Big Brother Watch and others v. the United Kingdom,* Appl. no. 58170/13, para 387.

requirements of prior suspicion and the level of judicial oversight. Mass surveillance is, by definition, untargeted, and to require reasonable suspicion would render the application of such a measure devoid of meaning.[55] That is why judicial control is possible only *ex post*. On the contrary, criminal investigations most frequently require an *ex ante* judicial warrant, grounded on concrete suspicion against an individual and after assessing the proportionality and necessity of the measure in relation to potential interferences with that individual's rights.[56]

3.2. *Covert Operations and Opaque Tools*

As already discussed, another challenge posed by digital investigative measures is their remote and covert application. Law enforcement authorities have the technical equipment, software and expertise to gain access to a person's IT system or to have their data processed by a high-risk AI system without that person's knowledge. The covert nature of these operations is largely driven by the need for law enforcement agents to maintain the advantage of surprise, taking into consideration factors like the volatile nature of digital data or the suspects' technical skills. Remote access and covert processing of data become a key to ensuring the integrity of criminal investigations.[57]

An example can be drawn from police hacking operations. As physical access is not necessarily required to install malware, the primary concern is that the covert and remote execution of the measure shields the targets from awareness, thus diminishing their ability to contest its lawfulness.[58] Secrecy enhances the effectiveness of law enforcement operations, yet it drastically impacts the fundamental rights of targeted individuals. Key details, such as how the investigation is conducted, its duration, the techniques applied and the system vulnerabilities exploited, are often not disclosed until the investigation is concluded, which means that individuals may not be aware that their rights have been infringed upon until much later.

Equally devoid of transparency is the application of high-risk AI systems for the purposes of evidence acquisition, crime investigation,

[55] *Ibid.*, para 317; *Centrum för Rättvisa v Sweden* (n 53), para 133.

[56] Bachmaier Winter (n 49), 9-10, using the traditional example of the interception of telecommunications.

[57] At this point, see Council of Europe's Report on 'The Deployment of Special Investigative Means' (2013), <www.coe.int/en/web/corruption/publications>.

[58] Gold and Latonero (n 15).

and prosecution. It is once again highlighted that most AI-driven tools are "black boxes" even for their deployers, meaning that law enforcement authorities are not often familiar with the way the algorithm processes data or produces its output.[59] Either crawling through publicly available online information or assisting in automated decision-making processes, the lack of transparency on how the tool works introduces significant concerns with respect to fundamental rights and the integrity of criminal investigations. After all, the possibility of producing biased, inaccurate or erroneous results is high, not only due to the input or training data but also because of a hidden feature of the algorithm itself.[60]

3.3. *Investigations Beyond Borders: Impact on Evidence Admissibility*

As previously stated, the increasing digitalisation of crime has reshaped the landscape of criminal investigations, particularly due to the growing transnational nature of crime and the decentralised nature of evidence.[61] As cybercrime spans national borders, traditional legal frameworks have proven inadequate for addressing the way evidence is collected and processed by law enforcement authorities. Especially within the EU, discrepancies in national laws concerning traditional investigative measures are further exacerbated by the lack of harmonised rules governing their application. Cross-border cooperation mechanisms, most notably the European Investigation Order, are often hindered by national rules on evidence acquisition and, subsequently, admissibility in court.[62]

[59] K. Quezada-Tavarez et al (n 42); S. Gless, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (2020) 51(2) *Georgetown Journal of International Law* 195, 217.

[60] Gless (n 59), where she notes that apart from the design of the algorithm, erroneous, imprecise or biased outputs can be the consequence of programming choices or the selection of input data.

[61] Bachmaier Winter (n 49), 10.

[62] Particularly interesting in this regard is the famous EncroChat case, which after long debates between German Courts reached the CJEU and its ruling on 30 April 2024. The case revolved around the transfer by means of European Investigation Orders (EIOs) of evidence collected by French and Dutch law enforcement authorities to their German counterparts, leading to trials against German citizens using EncroChat encrypted phones for illicit actions. The Regional Court of Berlin (Landgericht Berlin) questioned the lawfulness of the EIOs before the CJEU, pointing out that, among other issues, that the investigative measure ordered via EIO could not have been authorised in a similar domestic case. See, LG Berlin Request for a Preliminary Ruling (Beschluss vom 19.10.2022 - (525 KLs) 279 Js 30/22 (8/22)), openjur.de/u/2453066.html.

A prime example of the inconsistency in rules across the Member States concerns the designation of the competent authority responsible for the execution of investigative measures. The uncertainty often arising around whether the competent authority must be judicial in nature was addressed by the Court of Justice of the European Union (CJEU), which underlined that the interpretation of the term 'competent authority' is left to the national legislation of each Member State.[63] As a result, where a public prosecutor is empowered by national law to order a certain investigative measure in a domestic case, they are also considered a 'competent authority' in cross-border cases.[64] Consequently, a warrant by a judge is not always required.[65]

Other factors, such as ratione *materiae*, ratione *loci*, ratione *temporis* and ratione *personae*, also vary significantly from one Member State to another.[66] Divergences as to the legal grounds, geographical scope, duration and targeted person(s) of each investigative measure can lead to conflicts in cross-border investigations, as what may be permissible in one country may be illegal or result in inadmissible evidence in another. At this point, mutual recognition works as a valuable tool, preventing national authorities from blocking evidence obtained abroad from being presented in court, thereby having an impact on the acquittal or conviction of the defendant.[67]

While Member States have long been aware of the hurdles created by

[63] M. Böse 'Die Europäische Ermittlungsanordnung – Beweistransfer nach neuen Regeln?' (2014) 4 *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 153.

[64] CJEU, judgment of 27 May 2019, *Deutsche Staatsanwälte*, in cases C-508/18 and C-82/19 PPU, ECLI:EU-:C:2019:456, paras 42 et seq.; CJEU, judgment of 8 December 2020, *Staatsanwaltschaft Wien*, in the case C584/19, ECLI:EU:C:2020:1002, para 52; CJEU judgment of 30 April 2024, *M.N.*, in the case C670/22, ECLI:EU:C:2024:372, para 74.

[65] CJEU, judgment of 16 December 2021, *Spetsializirana prokuratura*, in the case C-724/19, EU:C:2021:1020, para 39; CJEU, judgment of 30 April 2024, *M.N.* (n 64), paras 75-77. In this regard, see also, A Kanakakis, 'Les droits des suspects ou des personnes poursuivies dans le cadre de la directive concernant la décision d'enquête européenne' (2024) 2 *Revue des Affaires européennes (RAE)* 289, 290.

[66] See, European Commission's Study on Cross-Border Use of Evidence in Criminal Proceedings (Final Report), 2023, 47 ff., highlighting the divergences in national legal frameworks.

[67] See, S. Allegrezza, 'Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality', in S. Ruggeri, *Transnational Evidence and Multicultural Inquiries in Europe*, (Springer 2014), 58; Allegrezza, 'Critical remarks on the Green Paper on obtaining evidence in criminal matters from one member state to another and securing its admissibility.' (2010) 9 *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 572.

the discrepancies between their national laws, they have shown reluctance to reevaluate traditional concepts, such as the territoriality principle (granting criminal jurisdiction to the state on whose territory the crime was committed)[68] or to promote a common or harmonised understanding of rules on evidence collection and admissibility.[69] Mutual recognition, even though established as *cornerstone* of the judicial cooperation in the EU,[70] is often seen as a way for Member States to prioritise their national legal systems instead of advancing towards a more integrated common area of freedom, security and justice.[71]

This unwillingness of EU Member States to adopt common rules on cross-border evidence was clearly demonstrated vis-à-vis the European Law Institute's Proposal on 'Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings', introduced in May 2023,[72] which was designed to address the urgent need for uniform standards for handling evidence, especially digital evidence, across the EU.[73] Despite the legal basis in Article 82 (2) (a) of the Treaty on the Functioning of the European Union (TFEU),[74] Member States still seem hesitant to give up control over such a sensitive area as criminal procedural law, especially admissibility of evidence, as they fear that adopting mutual rules might compromise

[68] See in this regard A. Payer 'The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries' (2023) 23 *International Criminal Law Review*, 178.

[69] Allegrezza (n 67).

[70] Presidency Conclusions of Tampere European Council, 15-16.10.1999, conclusion 33, <www.europarl.europa.eu/summits/tam_en.htm>.

[71] V. Mitsilegas, 'The constitutional implications of mutual recognition in criminal matters in the EU' (2006) 43(5) *Common Market Law Review*, 1277.

[72] Full text of the proposal available at <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>.

[73] L. Bachmaier Winter, 'Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?', (2023) 2 *eucrim*, 223-9, <eucrim.eu/articles/mutual-admissibility-of-evidence-and-electronic-evidence-in-the-eu-/#docx-to-html-fn6>.

[74] "To the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension, the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules. Such rules shall take into account the differences between the legal traditions and systems of the Member States. They shall concern: (a) mutual admissibility of evidence between Member States […]".

their national legal traditions and procedural safeguards, which are deeply ingrained in their legal systems.

With this background, one can imagine the true challenge for digital investigative measures, being incorporated in criminal procedural codes in EU Member States. Without harmonised rules for the application of these novel techniques in law enforcement settings, the acquisition of evidence both at national and at cross-border level is exposed, perhaps more profoundly than ever, to the challenge of evidence inadmissibility before national courts.

4. *Fundamental Rights Considerations*

As illustrated by the three examples used above, it is the very nature of digital investigative measures that raises considerable concerns about the fundamental rights of the person under investigation, particularly privacy, data protection and the right to a fair trial, as enshrined in Articles 8 and 6 of the European Convention on Human Rights (hereinafter ECHR) and Articles 7, 8 and 47 of the Charter of Fundamental Rights of the EU (hereinafter CFR EU), respectively.

Starting from the right to private and family life, it is already outlined how intrusive digital investigative methods can be in this regard. Automated collection of publicly available online information, remote searches and AI data processing for evidence acquisition purposes challenge the traditional understanding of privacy. Existing limitations as to the places and context of investigations are profoundly subject to transformation. An indicative example is the notion of 'home', which still remains the sacred site for private life expressions,[75] but is nowadays complemented by IT devices which increasingly host our private lives and follow their everyday expressions.[76] Consequently, this transformation in the traditional understanding of privacy calls for a reassessment of existing frameworks to ensure their continued relevance and appropriate application.[77]

[75] P. De Hert and S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E. Claes et al (eds) *Privacy and the Criminal Law* (Intersentia 2006), 61-104.

[76] U. Pagallo and S. Quattrocolo, 'The impact of AI on criminal law, and its twofold procedures', in W. Barfield and U. Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Elgar 2018), 385.

[77] P. De Hert and S. Gutwirth (n 75), 69.

Consistently addressing questions surrounding the lawfulness of state interference with privacy, the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU) insist on legality and necessity requirements. The interference must be hence provided by law and must be necessary in a democratic society, i.e. strictly necessary to achieve a legitimate aim, such as national security, crime prevention and the protection of the rights and freedoms of others.[78]

Furthermore, both Courts often underline the role of proportionality assessments in ensuring that any interference is not excessive in relation to the aim it serves.[79] However, the enhanced capabilities of new technologies have blurred the lines of what constitutes a proportionate intrusion, especially when these technologies can access and process unprecedented volumes of data. For this reason, the ECtHR has introduced two simple criteria for state interferences to be deemed lawful: accessibility and foreseeability.[80] Accessibility requires that individuals are able to have an indication of the legal rules applicable to the processing of their data (alternatively: that the processing is in accordance with the law). Foreseeability, on the other hand, ensures that they are able to foresee to a reasonable extent the consequences of such processing, which can also be supported by establishing transparency in how data was gathered.[81]

Failure to comply with these lawfulness requirements should amount to violations of the right to privacy as enshrined in the Convention and the Charter, and the evidence gathered thereof should be regarded as inadmissible. Consequently, their admission or role in the verdict would impair the individual's right to a fair trial. Nonetheless, the ECtHR has already made clear that the admission of pieces of evidence, whose collection contradicts to another guarantee of the ECHR does not

[78] CJEU, judgment of 16.12.2008, *Satamedia*, Case C-73/07, ECLI:EU:C:2008:727, para 56; CJEU, judgment of 6.10.2015, *Maximillian Schrems*, Case C-362/14, ECLI:EU:C:2015:650, paras 92-93; ECtHR, judgment of 6.09.1978, *Klass and others v. Germany*, App. no. 5029/71, para 42; ECtHR, judgment of 12.01.2016, *Szabo and Vissy v. Hungary*, App. no. 37138/14, para 73.

[79] See CJEU, judgment of 8.04.2014, Joint Cases C293/12 and C594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, where the Court established that the interferences with the rights protected in Articles 7 and 8 where not necessary (paras 51-65), but also not proportionate (para 69).

[80] ECtHR, judgment of 26 April 1979, *Sunday Times v. the United Kingdom,* App. no. 6538/74, para 49; ECtHR, judgment of 24 April 1990, *Kruslin v. France*, App. no. 11801/85, paras 27, 30; ECtHR judgment of 12 May 2000, *Khan v. The United Kingdom,* App. no. 35394/97, para 26.

[81] Critical remarks on accessibility, see De Hert and Gutwirth (n 75), 85-7.

automatically render the procedure unfair for the defendant.[82] Even by adhering to the 'fruit of the poisonous tree' doctrine, privacy violations by LEAs rarely amount to violations of Article 6 ECHR.[83]

As the violation of the right to privacy itself does not lead to fair trial infringements, the emphasis is placed upon the principles of adversariness and equality of arms, as two –closely linked with each other– components of the right to a fair trial. The content of these principles is summarised to the ability of each party in the proceedings to be given a reasonable opportunity to present their case under conditions that do not place them at a substantial disadvantage vis-à-vis their opponent.[84] Yet, as a prerequisite, the parties must be informed promptly about the allegations of their opponent,[85] in order to be able to comment effectively on them.[86] This "actual opportunity"[87] to challenge evidence suggested by prosecutors at court, relies then on the transparency of the method applied for evidence acquisition.

The complex balance between privacy, data protection rights and the principles of fair trial underscores why evidence collection with digital investigative measures must be accompanied by procedural safeguards. Commenting effectively on evidence reaching the court means being capable of questioning the reliability and accuracy of the collected data, while being informed about the collection and processing of those data. Without this foundational transparency, the integrity of the judicial process and the fairness of the trial are at risk.

[82] See ECtHR, judgment of 1.6.2010, *Gafgen v. Gemany*, App. no. 22978/05, in relation to Article 3 and 6 ECHR; ECtHR, judgment of 12.5.2000, *Khan v. the United Kingdom,* App. no. 35394/97.

[83] See also F. Verbruggen and C. Conings, 'After Zigzagging between Extremes, Finally Common Sense? Will Belgium Return to Reasonable Rules on Illegally Obtained Evidence?' (2021) 7(1) *Revista Brasileira de Direito Processual Penal*, 273; P. De Hert, 'Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)' (2019) *Brussels Privacy Hub Working Paper* 5/15, <brusselsprivacyhub.eu/-publications/wp515.html>.

[84] ECtHR, judgment of 7.6.2001, *Kress v. France*, App. no. 39594/98, para 72.

[85] Article 6 (3) (a) ECHR, referring to the right to a fair trial; More on its interpretation: C. Momsen and M. Willumat, 'Due Process and Fair Trial', in P Caeiro et al (eds), *Elgar Encyclopedia of Crime and Criminal Justice*, (Elgar 2024).

[86] CJEU, judgment of 2.3.2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C746/18, EU:C:2021:152, para 44; CJEU, judgment of 30.4.2024, *MN*, C-670/22, ECLI:EU:C:2024:372, para 105.

[87] See also ECtHR, judgment of 28.8.1991, *Brandstetter v. Austria*, App. no. 11170/84, 12876/87, 13468/87, para 67.

To uphold fair trial principles, it seems therefore possible to establish a clear regulatory link between national criminal procedural laws and already harmonised data protection rules and principles found in the General Data Protection Regulation (GDPR)[88] and the Law Enforcement Directive (LED)[89]. Adhesion to transparency, data quality, and data subject rights –including the rights to access, rectification, and erasure– might be the key to both effective and rights-compliant law enforcement when applying digital investigative methods.[90]

5. *Conclusions: Which Edge of the Sword Is Sharper?*

Arriving at the end of this paper, the "double-edged sword" riddle posed at the beginning resurfaces: whilst digital investigative measures offer unprecedented capabilities for crime prevention and investigation, they also pose formidable challenges. Law enforcement agencies are swiftly taking advantage of these novel methods, with their rush being somewhat understandable given the sophistication of contemporary crime. However, their actions are seldom guided by clear regulatory frameworks, raising significant concerns regarding the balance between effective law enforcement and the protection of fundamental rights.

The illustration of three core examples of digital investigative measures underscored a critical truth: the current landscape is marked by a disparity between expanded powers of law enforcement and protective measures available for individuals. As demonstrated, the distinction between

[88] 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).

[89] 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.

[90] Due to length constraints, a comprehensive analysis of these rules and principles lies beyond the scope of this study. For a more in-depth discussion, see P. De Hert, A. Kanakakis, J. Sajfert, 'Evidence Law, Data Protection Standards, and the Use of AI for Investigation and Prosecution', in K. Ligeti (ed) *AI Evidence and Criminal Proceedings* (Bloomsbury 2025) (forthcoming). Alternatively, relevant publications can be found within the framework of PROMODE research project.

proactive surveillance and reactive investigation may at times become unclear, potentially leading to abuse of mass surveillance practices that infringe upon privacy rights, while bypassing the necessary procedural guarantees. This lack of stringent oversight allows LEAs to operate with alarming latitude, often targeting individuals without any concrete suspicion of committing a crime.

The covert and transnational character of digital investigative techniques further complicates their application. Operating in secrecy, these methods impede individuals' ability to challenge evidence acquisition and assert their rights effectively. In addition, discrepancies among national laws not only obstruct effective cooperation among Member States but also expose individuals to a regulatory labyrinth, leaving them vulnerable to rights violations across jurisdictions.

Caught in this vicious circle, individuals find themselves unable to seek protection against fundamental rights infringements. As discussed, the admission of evidence obtained through privacy and data protection violations does not necessarily result in an unfair trial. Nevertheless, even when attempting to claim this "un-fairness", defendants often encounter insurmountable obstacles. They are frequently left in the dark regarding how evidence was collected, which severely restricts their ability to comment on or contest that evidence through judicial remedies.

In light of these considerations, the need for reforms in criminal procedural rules is clear and pressing, though the direction of such reforms is yet to be shown. Ultimately, the question of *which edge of the sword is sharper* becomes profoundly important. If left unaddressed, the balance of power will tilt dangerously in favour of law enforcement, eroding the safeguards meant to protect fundamental rights and freedoms. It is critical for lawmakers, at both EU and Member State level, to rise to the occasion, embracing a vision that not only empowers law enforcement agencies to combat crime effectively but also fiercely defends individuals' rights. Failure to do so risks entrenching a system where the sword of law enforcement cuts too deeply, leaving individuals vulnerable to, or worse, wounded by the omnipotence of state power.

Ophélie Sémiramis Medza-Mba*

The revival of media monopolies or the dilution of press pluralism. The French example in the light of the proposed law on audiovisual reform

"The press is against me, television is mine!" [1]

General Charles de Gaulle's statement about the press reflects the relationship that has governed the media and political power for many years. Far from being anodyne, this phrase sums up the place occupied by the State in the management of what is today considered by all to be the fourth estate.

Freedom of expression, which is one of the rights enjoyed by all human beings, is one of the so-called intellectual freedoms. Alongside other freedoms such as freedom of opinion and freedom of conscience, it is constitutionally recognized and guaranteed in all democratic republics. It is thus considered one of the fundamental pillars of democracy in a state governed by the rule of law.

In France, freedom of expression is recognized by article 11 of the 1789 Declaration of the Rights of Man and of the Citizen which states that: "The free communication of thoughts and opinions is one of the most precious rights of Man: every Citizen may therefore speak, write and

* Ph.D. student at the University of Reims Champagne-Ardenne, France.

[1] Quand De Gaulle invitait pour la première fois la presse à l'Elysée, *Le Parisien*, April 28, 2019, <https://www.leparisien.fr/politique/quand-de-gaulle-invitait-pour-la-premiere-fois-la-presse-a-l-elysee-28-04-2019>.

print freely, except to be held accountable for the abuse of this freedom in the cases determined by the Law". These domestic provisions guaranteeing freedom of expression in France, and are reinforced by the provisions of the European Convention on Human Rights, article 11 of which states that: "1. Everyone has the right to freedom of expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected". Freedom of information and communication, a fundamental component of freedom of expression, therefore, constitutes a crucial element in the construction of a citizen's conscience and autonomy of thought, when this is achieved in compliance with the imperatives of neutrality, objectivity and pluralism through the press.

Freedom of information and communication is guaranteed by obligations such as media pluralism and independence, to ensure that citizens have access to a wide range of information. In France, these safeguards were established by successive laws reforming the audiovisual sector and gradually ending the media monopoly held by the French state through the ORTF (Office de Radiodiffusion-Télévision Française) until 1974. The break with this state monopoly in the media was made in the name of freedom of expression, under pressure from groups who wished to achieve a true democratization of the sector. This split not only gave rise to several private press groups but also encouraged the development of online media.

Faced with the exponential growth of private media organizations and online media, a draft law on audiovisual reform has been initiated, involving the merger of various key public media. The aim is to create a media *holding company* bringing together all public TV and radio channels.

This initiative, strongly encouraged by the former Minister of Culture Rachida Dati, was intended to represent a necessary evolution of the French media landscape, while positioning itself as a bulwark against esteemed competition born of the rise of online and private media alike. This audiovisual reform project, which was interrupted by the unexpected dissolution of the French National Assembly on June 9, 2024, by the President of the French Republic, has nonetheless left a sense of dissatisfaction among unions and the public. Indeed, the very nature of this project to merge public broadcasting entities raises significant concerns regarding the potential erosion of freedom of expression, press freedom,

and media pluralism, principles enshrined and upheld by French law.

While legitimate questions remain as to the ability of the various independent online media to provide quality, reliable information, or the need to face up to the competition they represent alongside private media groups, other pertinent questions may also emerge alongside these issues. Specifically, the compatibility of the notion of public service with the imperatives of competition, profitability and competitiveness, to the detriment of the requirements of objectivity and independence.

In the light of these many factors, several questions arise: would the resurgence of a state media monopoly still be compatible with the objectives of the media, or does it represent a danger for pluralism?

In this study, we will analyze the stakes involved in strong state intervention in the audiovisual media (1) and then address the possible dangers of a state monopoly position, given the democratic objectives attached to the media (2).

1. *The challenges of government action in the audiovisual media*

The provision of a state monopoly over the media was for a time the norm in France, due to the context of the post-war period (1.1.). Today, the question is once again being raised as to how to guarantee media objectivity in an era of growing private media and disinformation (1.2.).

1.2. *Media monopolization: A necessary tool for safeguarding and reclaiming the national information landscape*

Since the media are often considered the "fourth estate" in a state, it was essential, as with any sensitive area of governance, for them to be properly regulated in order to protect the fundamental interests of the state, especially those related to ensuring democracy. These monopolistic media situations are not unique to France; they have also existed and continue to exist in several European countries, such as Italy. As the guarantor of the nation's institutions, the State positions itself as the key overseer of this delicate field, which, if misused, could potentially destabilize the nation's core values. This was especially evident during World War II, when the French press was hijacked to serve Nazi and Vichy propaganda.

During the Liberation, the media also played a crucial role for the

Resistance fighters who were exiled. The French government at the time sought to avoid repeating past mistakes, focusing on better protecting the sector. In 1958, at the initiative of General de Gaulle, the monopoly on audiovisual media was established, a system that would endure due to the political context and the vision of the media's role within the state. This control would be gradually challenged starting in 1968[2].

The political forces of the time sought to establish safeguards around the press and the power it wielded by placing the audiovisual sector under the supervision of the Minister of Information. French Radio and Television were officially recognized as public establishments of industrial and commercial nature, fully managed by the state. Given the inability of political powers to control the emerging online press, which was too diverse and critical of the government, General de Gaulle viewed the audiovisual media as a more malleable tool to fulfill public service information missions.

In 1964, the Office de Radiodiffusion-Télévision Française (ORTF) was created, consolidating the state monopoly over the audiovisual landscape. Alain Peyrefitte, the Minister of Information at the time, designated ORTF as a public organization responsible for radio and television. This monopoly persisted in a politically charged context. Although opposition parties did not challenge the monopoly itself, they began to criticize the limited space they were given in the media and questioned the supposed objectivity of the public broadcasters.

The situation came to a head during the May 1968 demonstrations, when opposition parties felt increasingly sidelined and marginalized by the media. The role of the media in shaping political dynamics, influencing parties and candidates, and swaying public opinion, became more apparent throughout the 1960s. The arguments that had justified the state monopoly began to lose traction, especially after the selective and biased media coverage of the events of May 68. The state's media were seen as serving the political majority in power, which further deepened the divide between the government and the opposition[3].

The commercialization of television, including the opening of public channels to advertising, contributed to a further loss of credibility for state-run media. Left-wing parties, particularly the Communists, viewed this as a betrayal of the public service mission, transforming it into a tool serving

[2] A. De Tarlé, "Chapitre 10 / l'État et les médias en France: Du service public au pluralisme libéral (1944-2009)"; Intelligences de la France Onze essais sur la politique et la culture, *Presses de Sciences Po*, 2010. p.209-230. CAIRN.INFO, <shs.cairn.info/intelligences-de-la-france--9782724611465-page-209?lang=fr>.

[3] *Ibid.*

the interests of an oligarchy[4]. The increasing dependence of audiovisual services on advertising revenues only reinforced these concerns[5].

This climate of suspicion culminated in the dissolution of ORTF in 1974[6], followed by the July 29, 1982 law, which proclaimed the freedom of audiovisual communication (Article 1). This marked the end of the French state's monopoly on the media and opened the sector to private competition. The new media landscape required greater regulatory power to ensure fair competition and protect public service principles.

1.2. *The need for State regulation in the face of growing private media power and online misinformation*

The access of private operators to public space, which began in the 1970s, expanded with the liberalization of the media. This proliferation of private media, coupled with technological advances, led to an increase in broadcasting channels, gradually relegating public media to a minority position in a highly fragmented media landscape.

As society's demands for informational content have grown, the justifications underpinning the establishment of a state monopoly have remained increasingly pertinent. All media, whether public or private, were still expected to adhere to press ethics, objectivity, and, above all, respect for pluralism. These principles eventually led to the creation of the Audiovisual and Digital Communication Regulatory Authority[7] (ARCOM), formerly known as the Higher Audiovisual Council[8] (CSA). ARCOM and the courts have already handled multiple cases brought by citizens and organizations in response to violations of professional ethics and media pluralism. Today, similar to the pre-World War I period, we are witnessing the resurgence of large private media groups, which raise concerns about potential collusion between these corporate giants and the state. This scenario echoes a discredited model seen in Italy, where MediaForEurope (MFE), a major private television group, founded by former Prime Minister Silvio Berlusconi, continues to challenge the

[4] *Ibid*; F. D'Almeida and C. Delporte, *Histoire des médias, de la Grande Guerre à nos jours,* Paris, Flammarion, coll. Histoire et actualité, 2010.

[5] Over the years, advertising contributions will rise to 25% of television revenues.

[6] S. Bachmann*, L'Éclatement de l'ORTF*, Paris, L'Harmattan, 1997.

[7] "*L'Autorité de Régulation de la Communication Audiovisuelle et Numérique".*

[8] "*Conseil Supérieur de l'Audiovisuel".*

state-owned RAI[9]. In France, a significant portion of the media is owned by private conglomerates, whose political leanings strongly influence social debates[10]. High-profile businessmen such as Vincent Bolloré, Martin Bouygues, and Bernard Arnault are among the prominent figures controlling these media outlets.

The rise of online media has further complicated the situation by creating a broad spectrum of content claiming to offer independent journalism. While some of these outlets do fulfill this role, the vastness of the digital world has led to problematic situations where the public is bombarded with an overwhelming amount of media and information. The line between genuine journalism and influencers masquerading as reporters has become increasingly blurred, posing significant challenges to the fundamental principles of objectivity and pluralism in the media. While traditional journalism relies on rigorous methods of fact-checking, neutrality, and the pursuit of balanced perspectives, the content produced by some influencers is often driven by commercial, personal, or ideological interests. This blending of roles obscures the distinction between factual information and promotional or subjective communication, undermining the reliability of sources and the transparency expected of media content. This situation weakens the public's ability to form an informed opinion by limiting access to critical and well-founded analyses.

In this context, where information overload and borderline illegal practices have emerged, the integrity of the media sector has suffered considerable damage.

Consequently, there is a growing need for legislative intervention to address the challenges posed by this environment. Some media platforms, particularly online, use advertising as a key revenue source, similar to the practices of the 1970s that were heavily criticized at the time. These commercial practices often shape the content of the information provided, with some content creators adjusting their political lines to cater to advertisers. This tacit submission to market forces and economic interests has an undeniable influence on the audience, which may be exposed to information whose authenticity and relevance are questionable. Furthermore, the recipient is often subtly encouraged to adopt consumer

[9] "Italie: le groupe de télévision MFE, contrôlé par la famille Berlusconi, a dépassé pour première fois la société publique RAI en termes de part d'audience en 2023", *La Correspondance de la Presse*, Lundi 22 avril 2024.

[10] "Capitalisme d'influence : enquête sur les grands barons de l'économie française", *Alternatives économiques*, 24 novembre 2023.

behavior[11].

The appeal of influencer marketing lies in its impressive return on investment, generating eleven times more profit than traditional advertising[12]. Yet, troublingly, 27% of sponsored content goes unmarked as such[13], deceiving audiences and eroding trust in media content.

This growing concern over deceptive practices has prompted the state, through legislative action, to set minimum standards for the creation of digital content. This ensures that consumers can clearly distinguish between genuine journalism and advertising. The Law of June 9, 2023[14], for instance, defines influencers as "individuals or legal entities who, for compensation, communicate content to the public via electronic means to promote goods, services, or causes." The law mandates that terms such as "advertising" or "commercial collaboration" must be prominently displayed in content to prevent fraudulent practices[15].

These violations are punishable under the French Consumer Code (articles L. 121-2 and L. 132-2). Within the European Union (EU), the Digital Services Act (DSA)[16], which was adopted on 19 October 2022, establishes a harmonised legal framework by imposing enhanced due diligence obligations on digital service providers. These include requirements relating to content reporting, transparency and consumer protection. The DSA constitutes a comprehensive regulatory response to the systemic risks posed by major online platforms within the EU's Member States[17].

---

[11] Numerous works have examined the issue of the shift between information content and propaganda in the manufacture of consent, See N. Chomsky, *La fabrication du consentement*, Agone Revised edition (16 octobre 2008); Edward Bernays, *Propaganda,* Paris, Éditions La Découverte, 2007, (1928).

[12] Figure given by B. Margaritelli, in "Influenceurs : quel cadre légal ?", *JSS n° 90*, 22 décembre 2021.

[13] *Ibid*.

[14] Law n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux.

[15] On this subject, see T. Girard-Gaymard, "Les influenceurs et le droit": *D. 2020*; E. Dumur and P. Wilhelm, "3 questions - Quel encadrement de l'activité et des pratiques des influenceurs ?" : *JCP*, 202 ; O. Boismery, "La responsabilité des influenceurs", *CCE,* 2022.

[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[17] *Le Règlement européen sur les services numériques (DSA) : protéger les droits des citoyens sur internet*, August 25th, 2023, Le Règlement européen sur les services numériques (DSA) : protéger les droits des citoyens sur internet | Arcom.

The DSA is a comprehensive regulatory response to the systemic risks posed by major online platforms in the EU. It aims to protect individuals from harm such as violations of human dignity, hate speech, harassment and the exposure of minors to harmful content, while also preserving the integrity of democratic institutions against disinformation, incitement to violence and foreign electoral interference. It thus seeks to balance the protection of public order and fundamental rights with the preservation of freedom of expression in the digital sphere[18].

The growing competition from private media and the opening of the online media sector, which has become a fertile ground for misinformation, have necessitated more direct state intervention. Whether through the creation of ARCOM or the introduction of standards for online media, the state's involvement in the media landscape has become essential. However, the state's intervention does not stop there; it is determined to regain a prominent role in the audiovisual sector, which has been weakened over the past few decades. This drive for renewed state control was evident when Olivier Véran, the then-government spokesman, expressed his desire to regulate online media, even suggesting the potential censorship of certain YouTube channels, in order to protect public service media from unfair competition.

Véran's comments revealed the government's intention to tighten its grip on the audiovisual landscape and, by extension, on the digital sphere, which is inherently free and volatile. His intervention provoked strong reactions from the online media, which felt directly threatened by such measures, as well as from the public, who perceived these remarks as reflecting an authoritarian shift in a government increasingly losing its grip on power[19].

2. *Deviances arising from monopolistic situations: a danger for pluralism and democracy*

In addition to being a threat to pluralism, media monopolization is just as great a threat to democracy. Firstly, it facilitates the establishment

[18] *Entrée en vigueur du DSA : une avancée majeure vers un internet plus sûr en Europe*, October 17th, 2022, Entrée en vigueur du DSA : une avancée majeure vers un internet plus sûr en Europe | Arcom.

[19] Numerous books brilliantly deals with these themes in depth, see: P. Bourdieu, *Sur la télévision*, Liber Raisons d'agir, 1996; S. Halimi, *Les nouveaux chiens de garde*, Liber Raisons d'agir, 2005.

of a dictatorship of one-track thinking (2.1.), and secondly, it contributes to the downgrading of the fundamental objectives of the right to information, making it subservient to issues that are more protective of market rules than of the general interest (2.2.).

2.1. *Monopolization of Media Discourse: the threat of one-track thinking*

When political power is at risk, or when faced with an authoritarian regime, the monopolization of media discourse can become a powerful tool to exert significant influence on public debate and current affairs. In several European countries, political ambitions surrounding media monopolies are becoming increasingly assertive. Italy serves as a particularly notable example, where the Prime Minister openly acknowledges using the media to advance her nationalist agenda[20]. Beyond dominating the media landscape, particularly the state broadcaster RAI, this agenda also involves taking control of strategic cultural sectors, demonstrating the far-reaching implications of such partisan ownership.

While some academics and journalists argue that this is not a new phenomenon, given Italy's longstanding media monopoly, the critical point remains that these media tools are being used for electoral propaganda. This raises profound questions about the necessity of media pluralism and the role of the State as a regulator and protector of the nation's broader interests, rather than merely safeguarding its own political and electoral objectives[21].

To prevent the return of a media monopoly, several mechanisms have been implemented in France. Some of these provisions originate from the Council of Europe and the European Union, while others are specific to the French and European legal systems. For example, French legislation, such as the 1986 Law, imposes restrictions on media concentration, aiming to preserve external pluralism—limiting the concentration of media power in the hands of a single entity, whether public or private. This law also enshrines the principle of media pluralism as a fundamental value.

In France, media pluralism is recognized as a constitutional objective. The French Constitutional Council has ruled that the free communication of thoughts and opinions would be ineffective if the public were unable

[20] "La reconquête culturelle rêvée de Giorgia Meloni", *La Croix n° 42728*, Mardi 26 septembre 2023, pp. 4 – 5; "En grève, les journalistes de la RAI refusent de devenir TV Meloni", *Le Nouvel Obs*, Lundi 6 mai 2024.

[21] "La reconquête culturelle rêvée de Giorgia Meloni", p. 4-5.

to access a sufficient variety of publications representing different perspectives[22]. This requirement compels the State to ensure that media entities meet certain criteria, such as diversity in broadcasting operators and the range of broadcasted content (external pluralism). Citizens can thus demand that the State take positive actions to ensure access to a variety of information sources.

In addition to Article 11-2 of the Charter of Fundamental Rights of the EU, which already affirms the obligation to respect the media and pluralism, the European Parliament adopted the Media Freedom Act (MFA) on 13 March 2024[23]. This legislation aims to strengthen the editorial independence of the media, protect journalists from political and economic interference, and ensure transparency regarding media ownership within the European Union.

European jurisprudence, particularly through the European Convention on Human Rights, also plays a significant role in ensuring respect for pluralism. For example, in the case of *Centro Europa SRL and di Stefano v. Italy* (June 7, 2012)[24], the Court reiterated the necessity of external media pluralism, stating that the State must intervene to prevent the creation of media monopolies. It further stressed that any public monopoly in the media should be equated with censorship.

In addition to external pluralism, mechanisms are in place to protect internal pluralism. One such mechanism is the establishment of independent financing tools to guarantee editorial freedom[25]. French jurisprudence, in alignment with European Convention on Human Rights standards, has reinforced the importance of internal pluralism, requiring media outlets to diversify the range of viewpoints they represent. This principle was emphasized in the *Council of State ruling in the Reporters sans frontières case* (February 13, 2024)[26].

Aware of the challenges posed by financing, new mechanisms have emerged to help media outlets maintain their independence from both

[22] Cons. const. 27 juill. 1982, n° 82-141 DC; See also: La Constitution et l'audiovisuel, *Nouv. Cah. Cons. const.,* n° 36, 2012.

[23] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

[24] Req. n° 38433/09.

[25] C. Broyelle, *Le pluralisme interne à la télévision et à la radio*, Légipresse, 2024 p.417; V. On this point, P. Auriel and C. Girard, "Le pluralisme des médias, condition de la liberté d'expression ?", *Revue des droits et des libertés fondamentaux,* 2020. Chron. 86.

[26] Req. n°463162.

political and economic pressures. For instance, media outlets seeking to remain independent can access participatory funding from internet users, associations, or trade unions, such as those offered by the *"J'aime l'info"* association or the *"Presse et Pluralisme"* association for print media.

The regulatory authority's control over pluralism is further evidenced by the Council of State's ruling on the speaking time of the President of the Republic. This ruling recognized that the President's television appearances could undermine media pluralism, especially in the context of electoral campaigns. The ruling emphasized that, in accordance with republican tradition, the President does not speak on behalf of any political party, and therefore his speeches should not be counted in the assessment of political pluralism in the media[27].

Beyond these challenges, the growing presence of economic giants in competition with the public sector, due to the liberalization of the media, raises more complex questions about the State's long-term role in this evolving landscape.

2.2. *The Progressive Alignment of Public Media with Market Logic: A Drift Away from Public Service Principles*

The issue of the independence of privately funded media first arose with the introduction of advertising into the media space. Over time, we have witnessed a gradual erosion of the fundamental objectives of public broadcasters' right to information, as the media landscape has been transformed in response to the growing dominance of private actors[28]. The rise of GAFAM (Google, Amazon, Facebook, Apple, Microsoft) and the proliferation of online platforms have significantly undermined the traditional audiovisual press sector. This disruption has highlighted the need for the State to intervene and restore balance to the financing of public audiovisual media.

However, any efforts to re-establish financial equilibrium would be better served by taxing the profits of these dominant tech companies rather than by penalizing competitive media outlets, which are unfairly

[27] CE, Ass., 08-04-2009 n° 311136.

[28] J. Bourdon, "Le service public de la radiotélévision : l'histoire d'une idéalisation en déclin", *Les Enjeux de l'information et de la communication*, 2013/2 (n°14/2), pp. 15 – 26 ; "Is public service broadcasting in terminal decline?", *BBC*, july 24, 2015, Is public service broadcasting in terminal decline? - BBC News ; M. Tracey, *The Decline and Fall of Public Service Broadcasting*, Oxford University Press, 1998 - 295 pages

blamed for the challenges faced by public media. The adverse effects of unfair competition from large private groups, combined with the growing influence of market-driven forces, have led to a noticeable decline in the quality of public media[29]. In pursuit of profit and ratings to mitigate financial losses, public broadcasters are increasingly prioritizing commercial objectives over their public service mandate. This shift away from their primary mission compromises their ability to serve the public good.

In response to this phenomenon, some media outlets are striving to preserve media pluralism by maintaining editorial independence. Acknowledging that media ownership is central to editorial control, independent journalists working for outlets such as *"Médiapart", "La Montagne"*, and "*Le Média"* have adopted various strategies to protect their editorial line from influence by powerful public or private entities[30]. These outlets have actively safeguarded their financial independence to avoid any possibility of being taken over by corporate or political interests.

Re-establishing a state monopoly over the media, particularly in the context of the current relationship between political powers and private media groups, would represent a regressive step. Such a move would inevitably result in ideological bias, collusion, and a return to the days when the public press was heavily influenced by business interests and foreign powers.

Given the immense power that the media wields in the political sphere – shaping public opinion and influencing political discourse – it is essential to recognize its role as a "fourth estate" and ensure its autonomy from other branches of government (legislative, executive, and judicial). While the State should remain a guarantor of media independence, it must do so without attempting to appropriate the media for itself. As the media environment evolves, however, the State's role is shifting. Is it moving from being merely a protector of public service to becoming an active defender of freedom of information, independence, and media pluralism in a landscape increasingly dominated by private interests?

[29] J. Bourdon, *Op.cit.*

[30] Chapter III «La sanctuarisation du capital des médias»*, in* J. Cagé & B. Huet*, L'information est un bien public,* Paris, Seuil, 2021, pp. 117-151.

Federico Di Silvestre*

States' Liabilities under Climate Finance Obligations

1. *Introduction*

Developed countries' commitment to provide financial resources to support developing countries' mitigation and adaptation actions constitutes a cornerstone to the achievement of UN Framework Convention on Climate Change ("UNFCCC") and Paris Agreement purposes on climate change (such financial resources are hereinafter referred to as "Climate Finance"). However, the specific features of such commitment remain debated. This lack of specificity makes it difficult to identify profiles of liability enforceable in practice vis-à-vis states that do not fulfil their commitment to provide Climate Finance. This paper will delve into a detailed analysis of developed countries' commitment to provide Climate Finance, with the aim of evaluating: (i) whether this commitment can be considered a binding legal obligation under international law; and (ii) what consequences a state may suffer in case of non-compliance.

2. *Obligations to provide Climate Finance under international law*

Climate Finance is the ensemble of the financial resources aimed at supporting developing countries' mitigation of greenhouse gas emissions and adaptation to the adverse effects of climate change.[1]

* Federico Di Silvestre earned his PhD at Roma Tre University.

[1] P.G. Ferreira, *Climate Finance and Transparency in the Paris Agreement. Key Current and Emerging Legal Issues*, Center for International Governance Innovation Papers,

The commitment to provide Climate Finance constitutes a subset of the more general legal category of financial obligations, which can be defined as a legal constraint between an owner of the obligation, who is bound to make a funding performance, and a beneficiary, who has the right to collect such funding.[2]

More in details, commitments to provide Climate Finance are legal constraints requiring developed countries to scale up financial flows to developing countries for specific climate-related projects aimed at promoting global decarbonization and climate resilience, in accordance with mitigation and adaptation goals envisaged by the UNFCCC and the Paris Agreement.[3]

The main sources of the commitment to provide Climate Finance are Articles 4.3 of the UNFCCC and Article 9.1 of the Paris Agreement.

Article 4.3 of the UNFCCC requires Annex II countries to supply developing countries with new and additional financial resources, to allow developing countries to meet the agreed full incremental costs of implementing climate mitigation measures. Under Article 4.4, Annex II countries shall also assist developing countries that are especially vulnerable to the adverse effects of climate change in meeting the costs of adaptation. Furthermore, Article 4.5 demands Annex II countries to finance technology transfer to developing countries.

From the 1992 UNFCCC to the 2015 Paris Agreement, Climate Finance provisions evolved.[4] Thanks to the 2009 Copenhagen Accord[5] and the 2010 Cancún Agreements,[6] the UNFCCC's provisions were significantly

n. 195, 2018, p. 3. In relation to the emerging of the issue of climate finance, see D. Bodansky, J. Brunnée, L. Rajamani, *International Climate Change Law*, OUP, Oxford 2017, p. 15.

[2] M. Rutzer Silvestre, *The Financial Obligation in International Law*, OUP, Oxford 2015, p. 20; Y. Yamineva, *A Legal Perspective on Climate Finance Debates. How Constructive Is the Current Norm Ambiguity?*, in B. Mayer, A. Zahar (eds.), *Debating Climate Law*, CUP, Cambridge 2021, p. 366.

[3] D. Rossati, A. Zahar, *Governing Climate Finance and Investment. The Role of Law*, in M. MEHLING, H. VAN ASSELT (eds.), *Research Handbook on Climate Finance and Investment Law*, Edward Elgar, Cheltenham 2022, p. 2, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4049282 (ultimo accesso 29 marzo 2025).

[4] For further details on this topic see Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., pp. 20-22.

[5] Decision 2/CP.15, The Copenhagen Accord, FCCC/CP/2009/11/Add.1 (30 March 2010) (Copenhagen Accord) paras 8–10.

[6] Decision 1/CP.16, The Cancún Agreements: Outcome of the work of the Ad Hoc Working Group on Long-term Cooperative Action under the Convention, FCCC/

clarified in relation to scale, balance and prioritization.[7] Specifically, developed countries committed to providing new and additional resources totaling almost 30 billion USD for the 2010–2012 period (also known as "fast-start finance") and to mobilizing 100 billion USD annually by 2020 from a variety of sources, including public and private, bilateral and multilateral to address the needs of developing countries (also known as "long-term finance").[8] The most at-risk developing countries, including least developed countries, small island developing states, and Africa, are entitled to receive priority for fast-start finance funding for adaptation.[9]

Moreover, two new organizations were formed: the Standing Committee on Finance, which was created to support the COP in leveraging climate finance, and the Green Climate Fund, which complements the already existing Global Environmental Facility, established in 1991, ahead of the 1992 Rio Earth Summit.[10]

The Paris Agreement introduced few substantial changes to the commitment to supply Climate Finance already envisaged by the UNFCCC. Article 9.1 requires developed countries to provide financial resources to support developing countries in fulfilling their ongoing obligations under the UNFCCC, both in terms of mitigation and adaptation.[11] Furthermore, under Articles 9.3 and 9.4, developed countries are demanded to take the lead in mobilizing wide varieties of sources of Climate Finance, with the aim of achieving a balance between adaptation and mitigation. Articles 9.5 and 9.7 place on developed countries the duty to biennially communicate

CP/2010/7/Add.1 (15 March 2011) (Cancún Agreements) paras 95–112.

[7] *Ibid.*

[8] *Ibid.*, paras 95, 98 and 99.

[9] *Ibid.*, paras 95 and 97.

[10] *Ibid.,* paras 102–112.

[11] The debate surrounding Article 9.1 of the Paris Agreement has been a contentious one for quite some time. Developed countries argued for broadening the scope of parties required to provide financial resources, including countries not traditionally considered developed but with sufficient resources to support both themselves and other developing countries. Conversely, others insisted that only a specific group of countries should bear this responsibility due to their historical contributions to climate change. Ultimately, the agreed upon text aims to widen the pool of providers assisting developing countries, acknowledging that many countries, including some major emerging economies, are already offering support through initiatives like the GEF and the GCF. See G. Gastelumendi, I. Gnittke, *Climate Finance (Article 9)*, in D. Klein, M.P. Carazo, M. Doelle, J. Bulmer, A. Higham (eds.), *The Paris Agreement on Climate Change. Analysis and Commentary*, OUP, Oxford 2017, pp. 243-244.

indicative quantitative and qualitative information related to the Climate Finance supplies and to provide transparent and consistent information on support for developing countries. Under Article 9, not only are developed countries expected to do their part. Indeed, Article 9.2 encourages also other parties to voluntarily provide or continue to provide Climate Finance to developing countries.[12]

It is still debated among legal scholars whether UNFCCC and Paris Agreement's commitments to provide Climate Finance constitute legal obligations under international law.[13]

Due to the partial vagueness of Article 4.3 of the UNFCCC and Article. 9.1 of the Paris Agreement, part of legal scholarship argued that such provision should not be considered as legal obligations, but rather simple political statements.[14]

However, from a hermeneutic point of view, in terms of prescriptiveness, the use of the word "shall" by both Articles provides a strong argument in favor of the existence of a legal obligation. [15]

Moreover, the prescriptiveness of the language of the provisions under analysis finds support not only from a purely literal reading, but also from

[12] According to part of legal doctrine, the main source of international law on Climate Finance is the Paris Agreement, which is the most recent and comprehensive treaty on climate law. Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 3. As a matter of facts, unlike the UNFCCC, the Paris Agreement explicitly refers to Climate Finance among its objectives. See Article 2(1)(c) of the Paris Agreement: "This Agreement, in enhancing the implementation of the Convention, including its objective, aims to strengthen the global response to the threat of climate change, in the context of sustainable development and efforts to eradicate poverty, including by: [...] Making finance flows consistent with a pathway towards low greenhouse gas emissions and climate-resilient development". In addition, the commitment made by developed countries to support developing countries financially was a key component of the agreement that allowed the Paris Agreement to be almost universally ratified in 2015. See Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 1.

[13] Yamineva, *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 366.

[14] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 5. See also A. Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, *Transnational Environmental Law*, 9(1), 2020, p. 179, arguing that "the Paris Agreement, while it does create a collective obligation in form, does not make it a legal obligation with legally binding force in substance. It therefore subsists at the level of an aspiration, albeit a very important one".

[15] For a more in-dept overview of the concepts of prescriptiveness of the provisions of the Paris Agreement see R. Bodle, S. Oberthür, *Legal Form of the Paris Agreement and Nature of Its Obligations*, in D. Klein, M.P. Carazo, M. Doelle, J. Bulmer, A. Higham (eds.), *The Paris Agreement on Climate Change. Analysis and Commentary*, OUP, Oxford 2017, p. 49.

a systematic interpretation. Indeed, it is worth noting that Article 9(2) of the Paris Agreement provides that parties different from developed countries "are encouraged" to provide financial support to developed countries. The term "are encouraged" clearly shows the non-binding nature of this provision.[16] Similarly, Article 9(3) of the Paris Agreement states that developed countries "should" continue to take the lead in the mobilization of climate finance. The replacement of the term "shall" with should" leaves no doubt that Article 9(3) of the Paris Agreement does not constitute a legally binding obligation.[17] Conversely, the vocabulary used in Article 9(1) of the Paris Agreement and Article 4.3 of the UNFCCC, i.e. the term "shall", is the same as that found in Articles 9(5) and 9(7) of the Paris Agreement on financial reporting, which are peacefully recognized as having the status of a legal obligation.[18] Therefore, it seems reasonable to conclude that the use of the term "shall" instead of the softer "should" or "are encouraged to" is a solid evidence of the intention to attribute to Article 9(1) of the Paris Agreement and Article 4.3 of the UNFCCC the standing of legal obligation.

Furthermore, the status of legal obligation of Article 4.3 of the

[16] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 5; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 5; M. Wewerinke-Singh, C. Doebbler, *The Paris Agreement. Some Critical Reflections on Process and Substance*, *University of New South Wales Law Journal*, 39(4), 2016, p. 1506.

[17] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 6.

[18] Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 247-249; Zahar A. (2016). The Paris Agreement and the Gradual Development of a Law on Climate Finance. Climate Law 6(1-2), 83-89; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 11. Every two years, developed countries are expected to submit reports outlining their plans to raise climate money, including the "projected levels of public financial resources to be provided to developing country Parties". See Paris Agreement, Art. 9(5). A developed country's "support" for developing countries, measured in terms of public funds used or successful private investment generated by public interventions, must be disclosed in the same biennial report. Reporting guidelines issued as CMA decisions under the Paris Agreement must be followed in full. See Paris Agreement, Art. 9(7). Moreover, every report needs to be reviewed by technical experts. See Paris Agreement, Arts. 9(7) and 13(13), leading to Paris Agreement CMA, 'Decision 12/CMA.1, Identification of the Information to Be Provided by Parties in Accordance with Article 9, Paragraph 5, of the Paris Agreement', UN Doc. FCCC/PA/CMA/2018/3/Add.1 (19 March 2019), Annex (hereafter 'Decision 12/CMA.1'), and Paris Agreement CMA, 'Decision 18/CMA.1, Modalities, Procedures and Guidelines for the Transparency Framework for Action and Support Referred to in Article 13 of the Paris Agreement', UN Doc. FCCC/PA/CMA/2018/3/Add.2 (19 March 2019), Annex, Part V (hereafter 'Decision 18/CMA.1').

UNFCCC and Article 9.1 of the Paris Agreement is acknowledged also by an authoritative part of legal scholarship.[19]

Nevertheless, a legal theory still maintains that, even if it were accepted that Article 4.3 of the UNFCCC and Article 9.1 of the Paris Agreement are legally binding obligations, their precise content would remain indeterminate, because the specific duties of each obligation's recipient are not precisely defined. Such indeterminacy would make such Climate Finance commitments, even if legally binding, unenforceable in practice.[20]

Following paragraphs will therefore focus on assessing whether or not the treaty provisions under analysis are detailed enough to generate obligations enforceable in practice under international law.

3. *The parties of the Climate Finance obligations*

Under both the UNFCCC and the Paris Agreement, beneficiaries of the obligations to provide Climate Finance are states not included in Annex II,[21] giving priority to countries that are especially vulnerable.[22]

[19] Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 243, stating that "the text that was finally agreed as Article 9.1 establishes a solid obligation for developed country parties to provide financial resources to developing countries. It is worth noting that the phrase 'in continuation of their existing obligations under the Convention' may be interpreted as a restatement of the obligation of developed country parties to provide financial resources to developing country parties, as stipulated in Article 4.3 of the Convention. In other words, it could be argued that Article 9.1 is not creating a new obligation for any party".

[20] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 5. For an overview of accountability of the subjects of international law for their acts and omissions related to climate change see Voigt C. (2021). International Environmental Responsibility and Liability. In L. Rajamani, J. Peel (eds.), *The Oxford Handbook of International Environmental Law*, OUP, Oxford 2021, pp. 166-183.

[21] The UNFCCC and the Paris Agreement identify "developing countries" as the recipients of the obligation to provide Climate Finance. The treaties do not explicitly identify the states that can be classified as "developing countries". However, this category can be delimited by reasoning *a contrario* starting from the definition of Annex II "developed countries" required to provide Climate Finance. See F. Yamin, J. Depledge, *The International Climate Change Regime. A Guide to Rules, Institutions and Procedures*, CUP, Cambridge 2004, p. 273; Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 370.

[22] Article 4(8) of the Convention lists eight categories of countries with 'specific needs and concerns' arising from the impacts of climate change or from a high dependence on income from, or consumption of, fossil fuels. The Paris Agreement is more laconic,

Regarding the position of the owner of the obligation, the UNFCCC places the obligation to provide Climate Finance on Annex II parties. Differently, the Paris Agreement refers, more generically, to "developed country Parties", but it does not identify which countries shall be considered as "developed countries".[23] This lexical change indicates Paris Agreement's intention of expanding the owners of the commitment to provide Climate Finance from Annex II countries to all countries that can be considered "developed".[24]

However, while on the one hand it would be fair to argue that, with the entry into force of the Paris Agreement, "developed countries", regardless of whether they are Annex II parties or not, are considered the owners of the climate finance obligation, on the other hand, it is still debated whether

stating, at Article 9(4), that the provision of climate finance should aim to achieve the priorities and needs of developing countries, 'especially those that are particularly vulnerable to the adverse effects of climate change and have significant capacity constraints, such as the least developed countries and small island developing States'.

[23] According to Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 226, the term 'developing countries' was intentionally left open and undefined, in order to expand the pool of states from which developing countries could receive Climate Finance.

[24] A. Zahar, *Climate Change Finance and International Law*, Routledge, London-New York 2017, p. 77. This argument finds support in the circumstance that countries contributing to the Green Climate Fund (GCF) – one of the operating entities of the Convention's financial mechanism – go beyond those listed in Annex II. Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 368. In addition, other scholars argue that further evidence of the expansion of the number of states called upon providing Climate Finance can be found in Article 9(2) of the Paris Agreement, providing that "other parties are encouraged to provide or continue to provide such support voluntary". Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 244. Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 240, while recognizing the usefulness of this forecast which seeks to extend the group of donor countries, further acknowledges that this provision, which is silent on who should provide the support and instead encourages rather than mandates or recommends it, is far weaker than what developed countries had hoped for. See also Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 172, arguing that the combined disposal of Articles 9(1) and 9(2) of the Paris Agreement expands the obligation to provide Climate Finance on all parties that actually are in a position to supply finance. However, it would be fair to note that if on the one hand Article 9(1) uses the language "shall", Article 9(2), on the other hand, provides that other Parties "are encouraged to", revealing its non-binding nature. Therefore, according to this reading, the obligation to provide Climate Finance remains placed on developed countries and cannot be extended to all countries capable in practice to provide such finance. Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 368-369.

Climate Finance obligations are individual or collective.[25]

According to some legal scholars, states are bound by two different categories of obligations under the UNFCCC and the Paris Agreement, namely: individual and collective obligations.[26]

Individual obligations are owned to a single state or to a group of states by an *individual* state.[27] Differently, collective obligations are placed on a *group* of states and require such a group, as a whole, to achieve a given task.[28]

Article 4.2 of the Paris Agreement, which mandates that states prepare, communicate, and maintain successive nationally determined contributions (NDCs) that they intend to achieve can be considered an example of individual obligation.[29]

[25] The existence of collective obligations under international law is still debated among legal scholars. See Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 165; Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 4-5.

[26] Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 138; Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 167; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 5; Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 369.

[27] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 4-5; Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 138. Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 369.

[28] Many scholars recognize the existence of collective obligations in the Paris Agreement and in international treaty law in general. See L. Rajamani, *The 2015 Paris Agreement. Interplay between Hard, Soft and Non-Obligations*, *Journal of Environmental Law*, 28(2), 2016, p. 343, stating that "It matters to whom the provision is addressed or who it identifies as actors. If the provision is addressed to "each Party", it denotes an individual obligation. If it is addressed to "all Parties", it could denote a collective obligation. If it refers to "Parties", in some cases, depending on the context, it could be a cooperative or collective obligation; in others, it could be a blanket or universal reference to "Parties", not necessarily signaling a collective or cooperative obligation"; C. Voigt, *The Paris Agreement. What Is the Standard of Conduct for Parties?*, *Questions of International Law*, 2016, pp. 17-18, arguing that 'some [treaty provisions] contain legally binding obligations, either of [a] substantive or of [a] procedural nature. Such obligations can be collective or individual'; Bodle and Oberthür, *Legal Form of the Paris Agreement and Nature of Its Obligations*, cit., p. 103, explicitly recognizing that the Paris Agreement contains collective obligations regarding finance. See also D. Bodansky, *The Legal Character of the Paris Agreement*, *RECIEL*, 25(2), 2016, pp. 145-147 and Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 18, 218–9, 225, 231, 234–235, 243, where the authors describe obligations as collective or individual.

[29] Another example is Article 4.3 of the Paris Agreement, stating that each Party's

Differently, Article 4.3 of the UNFCCC and Article 9.1 of the Paris Agreement, requiring developed countries to supply financial resources for developing countries, are examples of collective obligations.[30] Article 9.1 of the Paris Agreement, providing that developed countries shall supply financial resources to support developing countries' mitigation and adaptation efforts, preserved the nature of collective obligation already envisaged by Article 4.3 of the UNFCCC.[31]

This interpretation holds that Article 4.3 of the UNFCCC and Article 9.1 of the Paris Agreement establish an all-party collective obligation, meaning that those who can provide funding are obliged to do so, and those who receive funding are required to use it to improve their efforts at adaptation and mitigation.[32]

Given the existence of this collective obligation, failure to supply the required amount of Climate Finance would cause states holding such obligations to result collectively in breach of them.[33]

However, as further explained in the following paragraph 2.4, the difficulty in determining each state's share of the collective obligation creates substantial issues with enforceability. As a matter of fact, collective obligations require a rule for the division of labor to be agreed upon among the collectively obligated states.[34] Nonetheless, the UNFCCC, the Paris

successive nationally determined contribution will represent a progression beyond its then-current nationally determined contribution and reflect its highest possible ambition. Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 167.

[30] Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 5.

[31] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 4-5; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 5.

[32] Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 172.

[33] Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 175, also adding, in terms of consequences in case of breaches of these kinds of obligations that: "a community of states that breaches its legal obligation" […] "will suffer negative reputational consequences that are likely to call into question the notion of an 'international community', international law, and of course the climate change regime itself".

[34] *Ibid.*, 179, claiming that an "individuation mechanism" is required "in order to derive individual state obligations from its collective […] aim". See also A. Thompson, *The Global Regime for Climate Finance. Political and Legal Challenges*, in C. Carlarne, K.R. Gray, R. Tarasofsky (eds.), *The Oxford Handbook of International Climate Change Law*, OUP, Oxford 2016, p. 18, suggesting that states should agree on a mechanism for setting

Agreement or any other documents issued by subsequent COPs do not establish a clear rule to determine each developed country's contribution to the collective obligation to provide Climate Finance.[35]

4. *The subject-matter of the Climate Finance obligation*

Pursuant to both the UNFCCC and the Paris Agreement, the subject matter of the obligations to provide Climate Finance is, in general, the supply of financial resources. However, the precise feature of this obligation remains hard to define, specifically with reference to: (i) the exact focus of the financial obligation, (ii) the total amount of finance that developed countries shall provide, and (iii) the amount of finance that each developed country is expected to deliver.[36]

The correct focus of the financial support that developed countries are expected to provide remains debated. Under the UNFCCC, financial flows from developed countries shall aim at mitigation of climate change and adaptation to climate change's adverse effects.[37] Similarly, the Paris Agreement specifies that financial resources should aim to achieve a balance between mitigation and adaptation.[38] Treaties fail to clearly detail how an equilibrium between adaptation and mitigation shall be met, making it dif-

up each party' "fair share" of the obligation to provide Climate Finance.

[35] Yamineva, *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 369, also adding that any discussion aimed at degerming such a rule "would face strong political pushback from developed countries".

[36] The UNFCCC defines the finance to be provided as "new and additional". The rationale of this wording is to answer to the concern of developing countries, fearing that developed countries would simply divert money from already existing Official Development Assistance for climate purposes. See Yamin and Depledge, *The International Climate Change Regime: A Guide to Rules, Institutions and Procedures*, cit., p. 273. However, since the UNCCC does not define precisely that wording, it would be hard to assess if any amount of Climate Finance is actually "new and additional". Yamineva, *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 371. See also Wewerinke-Singh, and Doebbler, *The Paris Agreement: Some Critical Reflections on Process and Substance*, cit., p. 1506, claiming that Article 9 of the Paris Agreement is "consistent with article 4 of the UNFCCC, but does little to build on that text and even appears to backtrack by failing to mention that the finance from developed countries must be 'new and additional' as explicitly required by the UNFCCC.

[37] UNFCCC, Art. 4.

[38] Paris Agreement, Art. 9(4).

ficult to assess the correct proportion of each finance allocation.[39] However, it would still be possible to infer that climate finance shall support, in the most balanced way possible, both mitigation and adaptation.

Moreover, Climate Finance provisions require that, while providing for financial resources, developed countries shall take into consideration the needs of developing countries.[40] No further detail regarding such needs is directly provided. However, support in interpreting this provision can be found in Article 13.10 of the Paris Agreement, requiring developing countries to report on their financial support needs, providing the information detailed under Decision 18/CMA.1.[41]

In relation to the amount of finance developed countries are expected to mobilize, although the Paris Agreement does not define a precise scale, it clearly provides for a constant increase which should represent a progression beyond the collective goal of 100 billion USD a year by 2020, as previously provided for by the Copenhagen Accord and agreed to at COP 16, in Cancun.[42] The parties of the Paris Agreement are also required to establish an updated collective finance mobilization goal from a floor of 100 billion USD a year prior to 2025.[43] It would be fair to note, however, that according to scholars, due to the absence of settled accounting methodologies, it remains hard to determine if the mobilization goal has been successfully achieved. As a matter of fact, developing countries, civil society and academics often challenge the statistics on Climate Finance published by developed countries.[44]

Regarding the amount of finance each developed country is expected to provide, the UNFCCC and the Paris Agreement do not specify each state's share of the obligation, creating issues with the practical enforceability of

[39] According to some commentators, the term "balance" used by the Paris Agreement has the aims at correcting the current trend that sees financial flows for mitigation being substantially higher than those for adaptation. Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 245.

[40] Paris Agreement, Art. 9(4).

[41] Paris Agreement, Art. 13(10); Decision 18/CMA.1 (n. 25) section VI.C.

[42] UNFCCC Decision 1/CP.16 (2010), in UN Doc FCCC/CP/2010/7/Add.1.

[43] UNFCCC Decision 1/CP.21 (2015) [53], in UN Doc FCCC/CP/2015/10/Add.1.

[44] R. Weikmans, T. Roberts, *The International Climate Finance Accounting Muddle. Is There Hope on the Horizon?*, *Climate and Development*, 11, 2019, p. 100; Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 240. For a critical analysis of developed countries' non-fulfillment of their Climate Finance obligations see also N. Sachs, *The Paris Agreement in the 2020s. Breakdown or Breakup?*, *Ecology Law Quarterly*, 46(1), 2019, pp. 898-899.

the same.[45]

Nonetheless, the circumstance that an obligation is not directly actionable before a court does not inevitably make it a non-obligation.[46] Therefore, the vagueness of the provisions of Article 4.3 of the UNFCCC and of Article 9.1 of the Paris Agreement would not automatically prevent them from assuming the status of legal obligations.[47]

In addition, under the Vienna Convention on the Law of Treaties, state parties must implement in good faith every treaty in force upon them, regardless of the existence of a strong enforcement mechanism.[48] Accordingly, the practical unenforceability of Climate Finance provisions would not relieve developed countries of their obligation to implement them in good faith.

Consequently, in light of the above arguments, it can be inferred that: (i) Climate Finance must support, in a balanced manner, both adaptation and mitigation initiatives, taking into consideration the needs manifested by developed countries; (ii) the total amount of Climate Finance that developed countries are called upon to mobilize must be no less than 100 billion USD per year; and (iii) although it is unclear what amount of finance each state is required to provide, it remains understood that developed countries must still strive in good faith to reach the goal of collectively mobilizing 100 billion USD per year.

In addition, it is also worth observing that the obligation of states to struggle collectively to achieve the goal mentioned in point (iii) above finds its roots also in the general duty of cooperation envisaged under international climate law.

[45] Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 15; Yamineva Y., *A Legal Perspective on Climate Finance Debates: How Constructive Is the Current Norm Ambiguity?*, cit., p. 369.

[46] P. Sands, J. Peel, *Principles of International Environmental Law*, CUP, Cambridge 2018, p. 198, where the existence of non-actionable collective obligations is recognized.

[47] The opinion that Article 9(1) has legal content is shared, among others, by Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 240; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 2, stating that "the provision on Climate Finance remains a legally binding obligation for developed countries"; Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 243, claiming that "Article 9.1 establishes a solid obligation for developed country parties to provide financial resources to developing countries".

[48] Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), Art. 26. See also Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 3.

5. *Duty of cooperation under international climate law*

Cooperation among states is critical in the fight against climate change.[49] The crucial role played by cooperation is also recognized by the 2030 Agenda for Sustainable Development, pointing out that "the global nature of climate change calls for the widest possible international co-operation aimed at accelerating the reduction of global greenhouse gas emissions and addressing adaptation to the adverse impacts of climate change".[50]

All three of the main governing documents of the international climate change regime – i.e., the UNFCCC, the Kyoto Protocol, and the Paris Agreement – refer to cooperation.[51] A typical example is provided by NDCs, which are a cornerstone of the Paris Agreement.[52] Furthermore, developed countries are required by the UNFCCC and the Paris Agreement to assist developing countries in meeting their obligations by facilitating capacity building, providing financial support, and transferring technology to those countries.[53]

The development of the duty to cooperate in the context of

[49] As correctly noted by J. Rudall, *The Obligation to Cooperate in the Fight against Climate Change*, «International Community Law Review», 23(2-3), 2021, p. 184 "the effects of climate change will be felt by all states and combating climate change requires the efforts of every state". Moreover, "not all states have the resources to take the necessary measures to mitigate or adapt to the effects of climate change, while other states have the resources to do more in the fight against this common global challenge. Cooperation can help to bridge this gap". The need for a common and global response to the problems related to climate change is also acknowledged by D. Bodansky, *Climate Change: Reversing the Past and Advancing the Future*, «AJIL Unbound», 115, 2012, p. 80, stating that "climate change is the mother of all global common problems".

[50] Transforming our world: The 2030 Agenda for Sustainable Development, UN Doc. A/RES/70/1, 21 October 2015, para 31. The obligation to collaborate is also envisaged by an extensive array of global agreements, in addition to the case law and treaty provisions; for a general overview, see L. Boisson De Chazournes And J. Rudall, *Co-operation*, in J. E. Vinuales (eds.), *The UN Friendly Relations Declaration at 50*, CUP, Cambridge 2020, pp. 105-132.

[51] The UNFCCC makes reference to cooperation in many of its provisions, including its Preamble and Articles 3, 4, 5, 6, 7 and 9. The 1997 Kyoto Protocol addresses international cooperation in Articles 2, 10, and 13, and the 2015 Paris Agreement deals with it in its Preamble and Articles 6, 7, 8, 10, 11, 12 and 14.

[52] Similar to the UNFCCC, the Paris Agreement emphasizes that "climate change is a common concern of humankind" and that all states must take both individual and collective action to address it. See Paris Agreement, Preamble, para 11.

[53] See, for example, Article 4(1)(c), 4(3), and 4(5) of the UNFCCC; Article 9(1) of the Paris Agreement.

environmental protection and its integration with other obligations under international environmental law finds significant support in the work of international courts.[54] As a matter of fact, judges of the International Court of Justice (ICJ) have found that cooperation may necessitate that states exchange information, confer with the secretariat of an environmental treaty, or jointly assess the environmental impact of a particular activity.[55] Additionally, it has been noted that notification and consultation are additional aspects of the cooperation obligation.[56] The ICJ stated that "the obligation to inform … allows for the initiation of cooperation between the Parties which is necessary in order to fulfil the obligation of prevention".[57] The ICJ also observed that states ought to work together to prevent impeding the socioeconomic endeavors of the local populations residing in a particular area.[58]

Moreover, according to the International Tribunal for the Law of the Sea ("ITLOS"), "the duty to cooperate is a fundamental principle in the prevention of pollution of the marine environment".[59] The ITLOS further

[54] Rudall, *The Obligation to Cooperate in the Fight against Climate Change*, cit., p. 188.
[55] See, for example, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)*, Provisional Measures, Order of 8 March 2011 [2011] ICJ Reports 6.
[56] *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment [2010] ICJ Reports 14, para 77.
[57] *Ibid.*, para 102.
[58] *Case Concerning the Kasikili/Sedudu Island (Botswana v. Namibia)*, Judgment [1999] ICJ Reports 1045.
[59] *MOX Plant Case (Ireland v. United Kingdom)*, Provisional Measures, ITLOS Case No. 10, 3 December 2001, para 82. See also *Land Reclamation by Singapore in and around the Straits of Johor (Malaysia* v. *Singapore), Provisional Measures, Order of 8 October 2003, ITLOS Reports 2003*, p. 10, at p. 25, para. 92; *Request for Advisory Opinion Submitted by the Sub-Regional Fisheries Commission*, *Advisory Opinion, 2 April 2005, ITLOS Reports 2015*, p. 4, at p. 43, para. 140. In domestic courts, there has also been a consistent rise in climate-related litigation. For an overview, see United Nations Environment Programme, "The Status of ClimateLitigation: A Global Review" (2017). These cases were filed for a variety of reasons. In order to protect its citizens from climate change, the Dutch government was recently ordered by the country's courts to reduce emissions. See The Netherlands v. Urgenda, No. 200.178.245/01 (2018). The case was upheld by the Hague Court of Appeal on 9 October 2018 and the Dutch Supreme Court on 13 January 2020 (The Netherlands v. Urgenda, No. 19/00135). Notably, the courts ruled that the Dutch government's goals for reducing emissions needed to be more aggressive. They issued a warning, stating that the Dutch government had promised to take action through international treaties and that the threat posed by global warming is serious. One judge stated clearly that the state should not defend itself by claiming that Dutch efforts alone will not solve the world's climate crisis. Thus, rather than acting as a shield-to-shield states from accountability, cooperation can be used as a sword to force individual states to contribute more to the shared challenge of

elaborated this duty of cooperation in its Advisory Opinion in Case No. 31 of 21 May 2024, where the Tribunal took the chance to argue that states parties to the United Nations Convention on the Law of the Sea are required to "cooperate, directly or through competent international organizations, continuously, meaningfully and in good faith in order to prevent, reduce and control marine pollution from anthropogenic greenhouse gas ("GHG") emissions".[60] Furthermore in the same Advisory Opinion, the Tribunal added that states parties also have the obligation to "consult with one another in good faith with a view to adopting effective measures necessary to coordinate and ensure the conservation and development of shared stocks"[61] and "to cooperate in taking measures necessary for the conservation of living marine resources in the high seas that are threatened by climate change impacts and ocean acidification".[62]

In 2014, the International Law Association adopted its Draft Articles on Legal Principles Relating to Climate Change, containing the "foundational legal principles relating to climate change as well as to their inter-relationship", with the purpose of directing states' response to climate change.[63]

climate change. For further thoughts on climate litigation see M. Wewerinke-Singh, *State Responsibility, Climate Change and Human Rights under International Law*, Bloomsbury, London 2019; V. Tsang, *Establishing State Responsibility in Mitigating Climate Change under Customary International Law*, LL.M. Essays & Theses, 9, 2021.

[60] More specifically: "first, States Parties are required to cooperate in formulating and elaborating rules, standards and recommended practices and procedures, consistent with the Convention and based on available scientific knowledge, to counter marine pollution from such emissions. Second, States Parties are required to cooperate to promote studies, undertake scientific research, and encourage the exchange of information and data on marine pollution from anthropogenic GHG emissions, its pathways, risks and remedies, including mitigation and adaptation measures. Third, States Parties are required to establish appropriate scientific criteria on the basis of which rules, standards and recommended practices and procedures are to be formulated and elaborated to counter marine pollution from such emissions". ITLOS Advisory Opinion in Case No. 31 of 21 May 2024, para 321. See also R. J. Roland Holst, *Taking the current when it serves: Prospects and challenges for an ITLOS advisory opinion on oceans and climate change*, RECIEL, 31(2), 2022, pp. 217-225; Y. Tanaka, *The role of an advisory opinion of ITLOS in addressing climate change*, RECIEL, 31(2), 2022, pp. 206-216.

[61] ITLOS Advisory Opinion in Case No. 31 of 21 May 2024, para 411(f).

[62] *Ibid*.

[63] ILA, Declaration of Legal Principles Relating to Climate Change, Resolution 2/2014, Annex: Draft Articles on Legal Principles Relating to Climate Change, April 2014, Draft Article 1. These were arrived at following an analysis of jurisprudence, international treaties and state practice. See C. Schwarte E W. Frank, *The International Law Association's Legal Principles on Climate Change and Climate Liability Under Public International Law*, «Climate Law», 4(3–4), 2014, p. 202.

International cooperation is addressed by Draft Article 8, which requires states to cooperate in good faith with each other and with international organizations in order to "address climate change and its adverse effects". Particularly relevant for the purposes of this research is Draft Article 8.3, which, read in conjunction with Article 5.3, provides that international cooperation on climate change shall reflect the responsibility of developed countries to assist developing countries by providing financial assistance.[64]

As importantly, states' commitment to cooperate in the fight against climate change finds its roots also in various bilateral agreements entered into in the last decade.[65]

In light of the above, it can be argued that the obligation to cooperate finds specific application also in the framework of climate change law. The duty of cooperation entails both rights and obligations for states. Specifically, it requires developed countries to support, also financially, developing countries that lack the means to fulfill their responsibilities for mitigation and adaptation.[66]

[64] Draft Article 8 also lays out more focused types of cooperation, including enhancing scientific knowledge, developing emission reduction standards, adopting new legal frameworks, assisting developing countries where their capacity to respond to climate disasters is exceeded, and ensuring that international law is adequate in addressing the threat posed by climate change.

[65] EU-China Comprehensive Agreement on Investment (CAI), Agreement in Principle (2020), Section IV, Subsection 2, Article 6 *(a)* requires the signing parties to ""effectively implement the UNFCCC and the Paris Agreement adopted thereunder, including its commitments regarding its Nationally Determined Contributions". According to the EU-Canada Comprehensive Economic and Trade Agreement (2016), Article 24.9(2), parties committed to remove obstacles to investments of good and services relevant for climate change mitigation, with specific reference to renewable energy goods and related services. Also, the EU-Singapore Free Trade Agreement (2018), Article 7.3(1) contains provisions against the creation of obstacles to investment in renewable energy. In addition, the Japan-Switzerland Agreement on Free Trade and Economic Partnership (2009), Preamble, provides that the contracting parties are "determined in implementing this Agreement, to seek to preserve and protect the environment, to promote the optimal use of natural resources in accordance with the objective of sustainable development and to adequately address the challenges of climate change".

[66] Rudall, *The Obligation to Cooperate in the Fight against Climate Change*, cit., p. 189-190.

6. *The role of development-finance institutions in deploying Climate Finance*

Developed countries have been sending Climate Finance to developing countries both bilaterally and multilaterally for decades, despite the partially ambiguous treaty law on the subject.[67] A pivotal role for this achievement has been played by multilateral development banks (MDBs).[68]

[67] According to one count, the totals for bilateral and multilateral climate finance in 2019 were 29 and 34 billion USD, respectively. See Organization for Economic Co-operation and Development (OECD), *Climate Finance Provided and Mobilised by Developed Countries: Aggregate Trends Updated with 2019 Data* (OECD, 2021), p. 8. However, due to numerous data gaps and, more importantly, political and conceptual disagreements about what constitutes climate finance, the precise amount of climate finance provided for climate-sensitive development—that is, initiatives that lower emissions or support adaptation—will always be estimated differently, if not dispute. As a result, there is no consensus on the definition of climate finance. See R. Roberts – R. Weikmans, *Fragmentation, Failing Trust and Enduring Tensions over What Counts as Climate Finance*, in «International Environmental Agreements», 17 (2017), p. 131.

[68] For an overview of characteristics and operativity of multilateral development banks see I.U. Delikanli – T. Dimitrov – R. Agolli, *Multilateral Development Banks. Governance and Finance*, Palgrave Macmillan, London 2018, p. 10 and L. Engen – A. Prizzon, *A Guide to Multilateral Development Banks*, ODI Working Papers, London 2018, pp. 7-79. Because of the states' support they receive, MDBs typically borrow money at favorable rates from the private sector rather than transferring state-deposited funds. Organization for Economic Co-operation and Development (OECD), *Climate Finance Provided and Mobilised by Developed Countries: Aggregate Trends Updated with 2019 Data* (OECD, 2021), 9; Delikanli, Dimitrov, and Agolli, *Multilateral Development Banks: Governance and Finance*, cit., p. 13. MDBs then lend the borrowed funds to developing countries, as well as non-state actors operating within those countries, albeit at a marginally higher interest rate. See, for example, the Asian Development Bank's constitutive document, *Agreement Establishing the Asian Development Bank* (adopted on 4 December 1965, entered into force on 22 August 1966) 571 UNTS 23 Art. 11; Organization for Economic Co-operation and Development (OECD), *Climate Finance Provided and Mobilised by Developed Countries: Aggregate Trends Updated with 2019 Data* (OECD, 2021), 9; Delikanli, Dimitrov, and Agolli, *Multilateral Development Banks: Governance and Finance*, cit., p. 13-14. In general, these borrowers would not have been able to obtain fair market rates for their climate projects otherwise. See, for example, the Asian Development Bank's constitutive document, *Agreement Establishing the Asian Development Bank* (adopted on 4 December 1965, entered into force on 22 August 1966) 571 UNTS 23, Art. 14(v). For a practical example of MDB's commitment in the fight against climate change, see Asian Infrastructure Development Bank, et al., *The MDBs' Alignment Approach to the Objectives of the Paris Agreement: Working Together to Catalyse Low-Emissions and Climate-Resilient Development* (AIDB, 3 December 2018), p. 2: "We will strive to actively support low-emissions and climate-resilient development pathways through our interventions. To that end, we will further scale-up the provision of climate finance. We will operationalize new approaches to bridge the climate finance gap and accelerate the transition in order to effectively support

The majority of the multilateral Climate Finance and investment that developing countries receive is entrusted to MDBs.[69] Even though these institutions are not under the governance structures of the climate treaties, there is an exceptionally strong correlation between climate treaty provisions and the MDBs. The nature of the relationship is reflected in a statement made by nine MDBs during the 2018 UNFCCC COP 24 meeting. The MDBs reaffirmed their previously stated "vision to align financial flows with the objectives of the Paris Agreement" and committed to collaborating for the creation of a specific strategy constituting their tangible and continuing contribution to the implementation of Article 2.1(c) of the Paris Agreement.[70]

countries in achieving the goals articulated in their Nationally Determined Contributions (NDCs), including adaptation plans. We will go beyond current efforts to (i) prioritize, target and report on climate finance, (ii) mobilise private sector investments, (iii) support clients' access to concessional finance, including for leveraging private capital, and (iv) provide the needed technical assistance for climate action. We will do this in support of ambitions agreed to under the [UNFCCC]". See also B. Buchner et al., *Global Landscape of Climate Finance 2019*, Climate Policy Initiative, 2019, p. 5.

[69] Because the MDBs are not specifically named in climate treaties, the Global Environment Facility (GEF) and the Green Climate Fund (GCF) often take center stage. However, the combined amount of Climate Finance channeled through the GEF – which is associated with the climate treaties but not directly under their jurisdiction – and the GCF – which supports both the UNFCCC and the Paris Agreement – is far less than what the MDBs as a group are accountable for. See Global Environment Facility, *Report of the Global Environment Facility to the Twenty-Fifth Session of the Conference of the Parties to the United Nations Framework Convention on Climate Change*, UN Doc. FCCC/CP/2019/5 (26 August 2019), viii (for mitigation) and xi-xii (for adaptation); and Green Climate Fund, *Eighth Report of the Green Climate Fund to the Conference of the Parties to the United Nations Framework Convention on Climate Change*, UN Doc. FCCC/CP/2019/3 (2 September 2019), p. 1-2. Along with bilateral climate finance, the climate finance that crosses borders is the multilateral climate finance of the MDBs, GCF, and GEF (plus the trickle from the AF). It should be differentiated from domestically raised and spent funds, which are also occasionally referred to as climate finance. See Yeo S. (2019). Climate Finance: The Money Trail, *Nature*, 573, 32). The domestic component is significantly greater than the cross-border component by all estimates. See Buchner et al., *Global Landscape of Climate Finance 2019*, cit., p. 5. MDBs are therefore significant global participants in the Climate Finance framework, as argued also by L. Delina, *Multilateral Development Banking in a Fragmented Climate System. Shifting Priorities in Energy Finance at the Asian Development Bank*, in «International Environmental Agreements», 17 (2017), p. 76.

[70] Asian Infrastructure Development Bank, et al., *The MDBs' Alignment Approach to the Objectives of the Paris Agreement: Working Together to Catalyse Low-Emissions and Climate-Resilient Development* (AIDB, 3 December 2018), p. 1. Scholars suggest that the MDBs' solemnly declared close identification with the goals of the Paris Agreement suggests a power to move the law on finance and investment in a climate-friendly direction, thanks to

Thanks to MDBs, leveraged private capital will be increasingly associated with climate-sensitive global investments, in line with climate treaty objectives, while a declining percentage of private sector funding will support initiatives that harm the environment.[71]

7. *Conclusive thoughts*

It seems reasonable to argue that Article 4.3 of the UNFCCC and of Article 9.1 of the Paris Agreement place on developing countries a collective legal obligation to provide Climate Finance to developing countries.[72]

the fact that MDBs are independent, self-regulated organizations of considerable financial strength and consequence. Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., pp. 9-10.

[71] According to scholars, the main goal of MDBs changed from economic development to sustainable development a long time ago. See G. Handl, *The Legal Mandate of Multilateral Development Banks as Agents for Change toward Sustainable Development*, in American Journal of International Law», 92/4 (1998), p. 642. In light of the above, it is possible to argue that MDBs can outperform other financial institutions in terms of supporting climate-friendly finance for a number of reasons. Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., pp. 12-13. First off, the MDBs are free to compete in a "race to the top" since they are not subject to the same political constraints as states. Second, the primary goal of MDBs, which are autonomous and self-governing organizations, is to raise as much money and investment as possible for sustainable development. Furthermore, they collaborate and participate in normative convergence against a backdrop of largely minimal competition from one another. See Delikanli, Dimitrov, and Agolli, *Multilateral Development Banks: Governance and Finance*, cit., pp. 112: "While each MDB sets its rules of operation and governance, this is more a collective, rather than an individual process. MDBs usually operate in a similar manner, as a family of peer cross-referenced institutions adhering to common norms and standards, with large MDBs often acting as role models". Lastly, the conditions that MDBs place on loans establish a sort of global "common law" of sustainable finance and investment that applies to the developing world as a whole, which is now essentially the entire region in which MDBs operate. M.M. Mbengue – S. De Moerloose, *Multilateral Development Banks and Sustainable Development. On Emulation, Fragmentation and a Common Law of Sustainable Development*, in Law and Development Review, 10/2 (2017), p. 407.

[72] In relation to the legal nature of this commitment, firstly, the use of the word 'shall' by both Art. 4.3 of the UNFCCC and Art. 9.1 of the Paris Agreement is a clear indicator of the existence of a legal obligation. See Art. 4.3 of the UNFCCC and Art. 9.1 of the Paris Agreement. Furthermore, the circumstance that a provision of a treaty is not directly enforceable before a court of law does not, in itself, render that provision devoid of the qualification of a legal obligation. See Sands and Peel, *Principles of International Environmental Law*, cit., p. 198. Moreover, the status of legal obligation of both Art.

Regarding the focus of the obligation, it seems safe to say that Climate Finance shall support, in a balanced manner, both mitigation and adaptation projects, taking into due consideration the needs of the individual developing countries receiving the financial flows.[73]

However, in relation to the specific amount of money that shall be provided, while it is feasible to argue that developed countries should collectively mobilize no less than 100 billion USD per year,[74] it is currently neither defined nor definable with sufficient certainty what share of the obligation is due to each state.[75]

Nonetheless, under international law, states must implement in good faith every treaty provision applicable to them regardless of the existence of an effective enforcement mechanism.[76] Accordingly, developed countries bound by the UNFCCC and the Paris Agreement remain obligated to make reasonable efforts to provide, collectively, 100 billion USD of

4.3 of the UNFCCC and Art. 9.1 of the Paris Agreement is also recognized by highly qualified scholarly writings. Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 240 argues that "Article 9 obliges developed countries to provide financial resources to assist developing countries with adaptation and mitigation" and that this provision constitutes a "mandatory construction of [developed countries'] financial obligations"; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 2, states that "the provision on climate finance remains a legally binding obligation for developed countries"; Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 243, claims that "Article 9.1 establishes a solid obligation for developed country parties to provide financial resources to developing countries". With regards, instead, to the parties of the Climate Finance obligation, the position of the owner is taken by developing countries, giving priority to countries particularly vulnerable to the effects of climate change, while the owners of the obligations are, collectively, developed countries. Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 4-5; Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 5; Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 175. Consequently, in the event of non-fulfilment of this collective obligation, the states to which this obligation is addressed would be collectively in breach of it. *Ibid*.

[73] See Art. 4.1 of the UNFCCC and Art. 9.4 of the Paris Agreement. See also Gastelumendi and Gnittke, *Climate Finance (Article 9)*, cit., p. 245.

[74] UNFCCC Decision 1/CP.16 (2010), in UN Doc FCCC/CP/2010/7/Add.1 and UNFCCC Decision 1/CP.21 (2015) [53], in UN Doc FCCC/CP/2015/10/Add.1. See also Bodansky, Brunnée, and Rajamani, *International Climate Change Law*, cit., p. 240.

[75] Zahar, *Collective Obligation and Individual Ambition in the Paris Agreement*, cit., p. 15.

[76] Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), art 26. See also Ferreira, *Climate Finance and Transparency in the Paris Agreement Key Current and Emerging Legal Issues*, cit., p. 3.

Climate Finance to developing countries, regardless of whether or not the specific performance of this obligation has a high probability of being successfully enforced by developing countries before a competent court.

Furthermore, the duty of cooperation envisioned by international climate law contributes to giving legal foundation to developed countries' collective commitment to providing Climate Finance. Indeed, cooperation constitutes a key element of the UNFCCC, the Kyoto Protocol and the Paris Agreement.[77] Moreover, the importance of international cooperation among states in the field of environmental protection is acknowledged also by Article 8 of the 2014 International Law Association's Draft Articles on Legal Principles Relating to Climate Change[78] and by several judgements of international courts and tribunals.[79] From the foregoing, it would be possible to argue that, under international climate law, developed countries have a duty of cooperation requiring them to support developing countries that are unable to meet their obligations for adaptation and mitigation,[80] and the supply of Climate Finance in accordance with Article 4.3 of the UNFCCC and Article 9.1 of the Paris Agreement would constitute an effective example of such support.

To reinforce the validity and effectiveness of the obligation to provide Climate Finance, it is also worth mentioning the fact that, despite the partially ambiguous treaty law on the matter, developed countries have made use for decades of the mechanisms offered by the Global Environmental Facility, Green Climate Fund and Multilateral Development Banks to provide Climate Finance to developing countries on a bilateral and multilateral basis.[81] In addition, for their part, development-finance institutions also recognize their role in fulfilling the Climate Finance obligations placed on states by climate treaties.[82]

[77] The UNFCCC makes reference to cooperation in many of its provisions, including its Preamble and Articles 3, 4, 5, 6, 7 and 9. The 1997 Kyoto Protocol addresses international cooperation in Articles 2, 10, and 13, and the 2015 Paris Agreement deals with it in its Preamble and Articles 6, 7, 8, 10, 11, 12 and 14.

[78] ILA, Declaration of Legal Principles Relating to Climate Change, Resolution 2/2014, Annex: Draft Articles on Legal Principles Relating to Climate Change, April 2014, Draft Article 8.

[79] Rudall, *The Obligation to Cooperate in the Fight against Climate Change*, cit., p. 188.

[80] See, among others, ITLOS Advisory Opinion in Case No. 31 of 21 May 2024, paras 321 and 411. For an overview of other judgements see also Rudall, *The Obligation to Cooperate in the Fight against Climate Change*, cit., p. 189-190.

[81] Rossati and Zahar, *Governing Climate Finance and Investment: The Role of Law*, cit., p. 9-10.

[82] As demonstrated, for example, by Multilateral Development Banks' collective declaration

In light of the above, it could be considered demonstrated the existence, pursuant to the UNFCCC and the Paris Agreement, of a legally binding collective obligation for developed countries, concerning the supply of a total amount of 100 billion USD per year in favor of developing countries, to support the adaptation and mitigation goals that developing countries must achieve pursuant to the aforementioned international agreements.

However, the difficulties in enforcing this obligation remain. As a matter of fact, while on the one hand it could be practicable for developed countries, as a whole, to be considered in breach of their collective obligation, in the absence of clear criteria to define the amount of financial resources that each state should supply to reach the overall objective of 100 billion USD per year, it would currently remain particularly complex to define each state' share of responsibility.

To overcome this problem, it would be useful, first of all, to define more clearly which countries are bound by the obligation to provide Climate Finance, for example by updating Annex II of the UNFCCC and thus formalizing the expansion (already suggested from the Paris Agreement) of the group of owners of the obligation. Secondly, and above all, it would be desirable for the state parties to the Climate Finance treaties to define practical methods to define each state's share of the collective obligation to provide Climate Finance. Such an effort would undoubtedly be in line with developed countries' duty to cooperate and implement in good faith the treaty provisions they are bound to. Consequently, the chances for developing countries to assert their right to receive Climate Finance before a competent judicial body would be considerably facilitated. A similar strengthening of the obligation to provide Climate Finance would also constitute a solid catalyst to achieve the adaptation and mitigation objectives set out by the UNFCCC and the Paris Agreement.

during 2018 UNFCCC COP 24 meeting reaffirming their "vision to align financial flows with the objectives of the Paris Agreement". Asian Infrastructure Development Bank, et al., *The MDBs' Alignment Approach to the Objectives of the Paris Agreement: Working Together to Catalyse Low-Emissions and Climate-Resilient Development* (AIDB, 3 December 2018), p. 1.

Davide Sili*

The Co-Ownership of Jointly Developed Patents in the U.S., a Critical Analysis in the Light of Eco-sustainability

1. *Introduction*

Green innovation fits into the broader idea of sustainability, which includes not only environmental profiles, but also social and economic aspects. First of all, green innovation can be expressed through products, industrial or management processes capable of increasing resources efficiency. In particular:

> «Green innovation plays a key role in improving green growth performance by saving resources and reducing environmental pollution by increasing production efficiency, saving energy and reducing emissions»[1].

Then, the company that applies this innovation sees its economic power increase and, consequently, its inclination to invest and create employment[2]. In this regard Stojčić wrote appropriately:

* PhD Student at Roma Tre University.

[1] Z. Feng; W. Chen, *Environmental Regulation, Green Innovation, and Industrial Green Development: An Empirical Analysis Based on the Spatial Durbin Model*, in *Sustainability*, vol. 10, 2018, p. 4. See also Y. Sun et al., *Green Innovation for resource efficiency and sustainability: Empirical analysis and policy*, in *Resources Policy*, vol. 81, 2023, p. 2, especially when it is written that «green innovation can lead to a higher level of resource efficiency. Green innovation can seek to create a new process, technology, or organizational approach in many economic sectors to increase the efficiency of resources in an economy».

[2] «Our results from more than five thousand firms show a positive relationship between green innovation and employment, and the relationship is more pronounced for dirty industries». R. Kunapatarawong; E. Martínez-Ros, *Towards green growth: How does*

> «External eco-innovation incentives, whether public or private, motivate the search of firms for ways of achieving higher process efficiency and greater product value. Such actions yield an additional benefit by preventing socially undesirable underinvestment in innovations and an excessive amount of negative environmental externalities»[3].

The idea of green innovation has therefore introduced this virtuous dynamic into international trade: companies, aware of the consequences of their production processes on the environment, tend to include attention to green issues in their corporate strategies to gain a good reputation among their respective customers. Indeed, a commercial entity known for its environmental commitment has a better chance of attracting consumers, investors and talented employees. Therefore, the activity of companies in the creation of specific products, industrial processes, marketing techniques and corporate structures, can generate a reduction in human environmental impact compared to existing alternatives[4] and many other positive effects on society and, in general, on the economy.

However, individual action by companies does not seem sufficient to effectively promote green innovation. Indeed, green innovation, which progresses through complementary patents that belong to different entities, requires common action among companies[5] and the signing of

green innovation affect employment?, in *Research Policy*, vol. 45, 2016, p. 1227.

[3] N. Stojčić, *Social and private outcomes of green innovation incentives in European advancing economies*, in *Technoinnovation*, 2021, p. 3.

[4] See M. Baise; K. Rennings, *Lead markets and regulation: A framework for analyzing the international diffusion of environmental innovations*, in *Ecological Economics*, vol. 52, 2005, p. 6; K. Rennings, *Redefining Innovation – Eco Innovation Research and the Contribution from Ecological Economics*, in *Ecological Economics*, vol. 32, 2000, p. 322; P. Klemmer et al., *Environmental Innovation: Incentives and Barriers*, Analytica, Berlino 1999.

[5] «The systemic […] and complex character of environmental innovations suggest that, to develop them, cooperation may be even more important than when it comes to introduce other types of innovations. […] Furthermore, to carry out a product that reduces environmental impacts is a rather complex task and often requires information and skills distant from the traditional knowledge base of the industry. Eco-innovations represent a technological frontier on which firms are still inexperienced and market and technological uncertainties increase as there are no widespread-accepted standards either in terms of specific technological solutions or of measures to evaluate the environmental performance of products and processes». V. De Marchi, *Environmental innovation and R&D cooperation: Empirical evidence from Spanish manufacturing firms*, in *Research Policy*, vol. 41, 2012, p. 615. «Complexity represents a fundamental issue of green innovations, being these the result of the integration and combination of several and heterogeneous technologies and knowledge resources». A. Messeni Petruzzelli et al., *Organizational*

intricate patent pooling agreements. In this way, multiple parties, without incurring huge transaction costs, have the ability of accessing each other's technologies for a common purpose, such as Research and Development (R&D) collaborations[6]. The latter can end with the creation of individual patents or joint patents depending on whether or not the companies are able to distinguish the individual contributions in the final results.

As a matter of fact, the impact of R&D support on eco-sustainable innovation is expressed in two ways: 1) through the sharing of independent technologies capable of giving rise to new technological systems consisting of individually patentable inventions; 2) through processes in which the interconnections of the relevant technological components necessarily lead to a joint invention. For example, as a result of the first type of collaboration, there are photovoltaic technologies that, due to their modular nature, constitute the building blocks of many different conformations. As a result of the second type of collaboration there are green biotechnologies, which, due to the multiple and indistinguishable interdependencies between them within the innovative processes, necessarily lead to a unitary finding. In this regard, the following critical reading is interesting:

> «Green collaborative innovation refers to a new organizational approach to green innovation in which green innovation entities cooperate and jointly develop. This approach can fully unleash the vitality of the "human resources, capital information, and technology" elements among innovation entities, promote the effective convergence of innovation resources and elements, achieve mutual benefit through innovation, and thereby enhance enterprise value and core competitiveness […]. Joint patent applications capture the output of enterprise collaborative innovation»[7].

For jointly developed patents, the most advantageous practice for

Factors and Technological Features in the Development of Green Innovations: Evidence from Patent Analysis, in *Innovation*, vol. 13, n.3, 2011, p. 294.

[6] «Now, when exclusive IP rights are available over multiple, discrete complementary (and often minuscule) inputs, rather than over end products, exclusivity tends to "backfire". When the holders of IP rights over complementary items are more than two, the transaction costs required for their joint exploitations grow exponentially». M. Ricolfi, *The new paradigm of creativity and innovation and its corollaries for the law of obligations*, in P. Drahos et al. (eds.), *Kritika: Essays on Intellectual Property* (vol. 1), Edward Elgar Publishing, Chelthenam 2015, p. 165.

[7] J. Lian et al., *How green bonds promote firms' green collaborative innovation?*, in *Corporate Social Responsibility and Environmental Management*, vol. 31, n. 6, 2023, pp. 6-7.

companies is to conclude private ordering agreements that set out detailed provisions on the rights and obligations of the co-owners. In the absence of a specific agreement, the rights and obligations of the co-owners are subject to the default rules of each jurisdiction where the related patent is registered. In other words, the default rules are applicable when the parties do not contractually establish rules that differ from the discipline provided by law. In any case, if the parties do not initially establish their own contractual rules, they can do so at any time, even after the patent has been granted. However, private ordering agreements are not always feasible due to transaction costs. In such cases, the presence of jointly developed patents within a legal system is influenced by the default rules[8]. In the absence of a specific agreement between the parties, these rules apply to any case of patent co-ownership, including that of joint development, which characterizes eco-sustainable innovation.

More specifically, it should be considered that the default rules provide for numerous rights and obligations of the parties. Overall, the right to grant a non-exclusive license to third parties of the shared eco-sustainable patent appears to be the most useful to best exploit its environmental benefits. Indeed, the alternative of the exclusive license is very limiting for eco-sustainable patents. As evidence of this, the following critical reading is interesting:

> «One may, however, mention a particular risk that comes with exclusively licensing a technology with potentially large social and environmental impact to a specific company. If the technology has potentially multiple applications to benefit society, but the exclusive licensee uses only one or few of them, the technology is prevented from unfolding its full potential impact»[9].

[8] «The difference in patent law of each country influences the activities of enterprises for the joint R&D in such countries and accordingly influences the number of the joint patent application of the enterprises». T. Hashimoto et al., *Managing joint R&D: an investigation into joint patent applications in Japan, US and Europe*, in *International Journal of Technology Transfer and Commercialisation*, vol. 11, n. 3, 2012, p. 141. «Given the complexity and uncertainty surrounding joint patenting, it is rational for the companies to obtain co-owned patents in a situation where they will find effective patent protection». J. Hagedoorn, *Sharing intellectual property rights – An exploratory study of joint patenting amongst companies*, in *Industrial and Corporate Change*, vol. 12, n. 5, 2003, p. 1046. See also A. Fosfuri et al., *Shared Ownership of Intangible Property Rights: The Case of Patent Coassingments*, in *Journal of Legal Studies*, vol. 46, n. 2, 2017, pp. 353-354; A. Gorbatyuk, *The Allocation of Patent Ownership in R&D Partnerships: Default Rules v. Contractual Practices*, in *SCRIPTed*, vol. 17, 2020, pp. 4-53.

[9] P. Vimalnatah et al., *IP Strategies for Green Innovations - An Analysis of European Inventor Awards*, in *Journal of Cleaner Production*, 2022, p. 11

In this regard, the article first aims to critically examine the default rules for non-exclusive joint patent licensing in the United States, considering the uniqueness that this presents compared to the equivalents of other national systems. Secondly, it intends to understand whether such uniqueness favor or hinders the creation of eco-sustainable shared patents.

2. *The U.S. system of default rules in joint patent non-exclusive licensing*

The default rules in the United States on joint patents can be found in Title 35 of the United States Code. In this regard, it should be noted that many of them have been subsequently implemented by case law over the years.

In any case, the starting point is represented by the concept of joint patent. This means that at least two different applicants who have jointly applied for a patent application are required.

In this regard, Section 116, point (a), states:

> «(a) Joint Inventions. When an invention is made by two or more persons jointly, they shall apply for patent jointly and each make the required oath, except as otherwise provided in this title. Inventors may apply for a patent jointly even though (1) they did not physically work together or at the same time, (2) each did not make the same type or amount of contribution, or (3) each did not make a contribution to the subject matter of every claim of the patent».

More specifically, the joint applicants are co-owners of the joint patent and each of them has undivided ownership of the entire patent. In this context, the U.S. legal system, particularly attentive to protecting private property, allows each joint owner to act independently, unless there are different agreements. More specifically, Section 262 establishes that:

> «In the absence of any agreement to the contrary, each of the joint owners of a patent may make, use, offer to sell, or sell the patented invention within the United States, or import the patented invention into the United States, without the consent of and without accounting to the other owners».

Accordingly, under Section 262 of Title 35 of the United States Code, each co-owner can exploit the patent independently. Case law included the

right to grant it in non-exclusive license to third parties without having to obtain the consent of the other co-owners[10] and without having to share the proceeds of the license with them.

This practice in the United States is unique among both common law and civil law systems, as well as in Asian countries.

In the United Kingdom, for example, Section 36(3)(b) of the Patents Act (1977) states that no co-owner can grant a patent license without the consent of the others. The same is stated in Australia by Section 16(1)(a) of the Patents Act (1990). In Canada, this issue is governed by case law. In *Forget v. Specialty Tools of Canada Inc.* (1995), the Court of Appeal of British Columbia stated that a co-owner cannot, without the consent of the others, grant the joint patent license to third parties, otherwise it would have the effect of diluting the rights of the other co-owners[11].

In this sense, civil law systems are in line with common law systems, as demonstrated, for example, by the Article XI 49 § 1-2 of the Belgian Code of Economic Law. It states that in the absence of a different agreement among co-owners, no one is authorized to grant any type of license to third parties without the consent of all others[12].

In Germany, the joint patent licensing to third parties is somewhat controversial, as the rules concerning patent co-ownership are not governed by an *ad hoc* provision. More specifically, Sections 741-758 BGB do not only apply to joint ownership of tangible goods, but also to joint ownership of patents, trademarks and utility models. Instead, the joint ownership of a copyright is regulated by an *ad hoc* provision, i.e. by Section 8 of the German Copyright Act[13]. Anyway, as for to joint patent licensing, accordingly to § 743 (2) BGB, the prevailing doctrinal opinion holds that:

[10] «[A co-owner] may make use of and sell specimens of the patented invention and may license others to do so; and neither he nor his licensees can be enjoined from a continuance in so doing». *Talbot v. Quaker State Oil Refining Co.*, 28 F. Supp. 544, 548 (W.D.Pa.1938). «[…] a co-owner of a patent can even grant a license to a third party without consent of the other owners». *Willingham v. Star Cutter Co.*, 555 F.2d 1340, 1344, 194 USPQ 249, 253 (6th Cir.1977). «[…] unless the co-owner has given up [its] rights through an "agreement to the contrary", the co-owner may not be prohibited from exploiting its rights in the patent, including the right to grant licenses to third parties on whatever conditions the co-owner chooses». *Schering Corp. v. Roussel-UCLAF SA*, 104 F. 3d 341 (1997), 344.

[11] *Forget v. Specialty Tools of Canada Inc.* (1995) 62 CPR (3d) 537, para 20.

[12] Similar *ad hoc* regulations can be found in other European systems. See, for example, art. 66, paragraph 2, of the Dutch Patent Act or Article 72, paragraph 3, of the Spanish Patent Act.

[13] <https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html>.

> «Each part-owner is authorized to use the joint invention only to the extent that the use by other part-owners is not impaired. Notably, however, "use" of the invention does not encompass licensing of the invention, which would therefore require approval by the other part-owners in accordance with § 747 S. 2 BGB. In the case of a "community of joint owners" (*Gesamt-handsgemeinschaft*), all part-owners need to agree on the modus of exploitation of the joint invention»[14].

The same logic can be found in non-Western contexts, as demonstrated by Article 99, paragraph 4, of the South Korean Patent Act[15] and Article 73, paragraph 3, of the Japanese Patent Act[16].

As is evident, the most common position among different patent systems is to allow granting joint patent license by the co-owner, whether exclusive or non-exclusive, only with the consent of all co-owners. Therefore, such models provide for veto power for each co-owner and are called veto-power systems.

Some similarities with the U.S. model can be found in China and France, especially regarding the freedom of each co-owner to grant a non-exclusive license of the joint patent.

Article 14 of the Chinese Patent Law establishes:

> «Where the co-owners of a patent application or patent have concluded an agreement on exercising of the right, the agreement shall apply. In the absence of such agreement, any co-owner may independently exploit the patent or license another party to exploit the patent through non-exclusive license; any fee for the exploitation obtained from licensing others to exploit the patent shall be distributed among the co-owners. Except for the circumstances as provided in the preceding paragraph, a jointly owned patent application or patent shall be exercised with the consent of all co-owners»[17].

---

[14] B. Banks et al., *Dealing with Joint Intellectual Property Ownership in the US and Germany*, in *DAIJV Newsletter*, vol. 36, n.2, 2011, p. 60.

[15] «Where a patent right is jointly owned, an owner may not grant an exclusive license or a nonexclusive license of the patent right without the consent of the other owners». <https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/kr/kr041en.pdf>.

[16] «If a patent right is jointly owned, no joint owner may establish an exclusive license or grant a non-exclusive license on the patent right to any third party without the consent of all the other joint owners». <https://wipolex-resources-eu-central-1-358922420655.s3.amazonaws.com/edocs/lexdocs/laws/en/jp/jp262en_1.pdf>.

[17] <https://www.unitalen.com.cn/xhtml/report/16124419-1.htm>.

Article L. 613-29, point (c), of the Intellectual Property Code in France provides:

> «Each of the joint owners may grant to a third party a non-exclusive licence to exploit the invention for his own benefit, subject to equitable compensation of the other joint owners who do not personally exploit the invention or who have not granted a licence to exploit it. In the absence of an amicable agreement, such compensation shall be fixed by the court»[18].

In both China and France, the freedom of each co-owner to grant a non-exclusive license to the joint patent is counterbalanced by the burden of attributing compensation to the others. This burden, however, is not found in the U.S. legal system.

The high level of freedom typical of the U.S. model is explained by the maximum valorization of the individual position of each co-owner of the joint patent, as traditionally supported by federal jurisprudence. In *Blackledge v. Weir & Craig Mfg. Co.* (1901), for example, the Court of Appeal for the 7th Circuit stated that:

> «There can be no accountability on […] a part owner […] to other owners for profits made by the exercise of his individual right, whether it be by engaging in the manufacture and sale, or by granting to other licenses, or by assigning interests in the patent. His use of the invention in any lawful way is not an appropriation of anything which belongs to another. The separate rights of the other owners remain unaffected. They are equally free to use the invention in all legitimate ways for their individual profit»[19].

Based on this precedent, the U.S. courts[20] recognized the co-owner's right to license the joint patent, but «this right to license does not extend to the granting of an exclusive license by one of the co-owners without the consent of the other owner or owners»[21]. Indeed,

> «it is clear that one of the patentees can not grant what does not belong to him, and if he gives a license or makes a contract for the use

[18] <https://french-business-law.com/french-legislation-art/article-l613-29-of-the-french-intellectual-property-code/>.

[19] *Blackledge v. Weir & Craig Mfg. Co.*, 108 F. 71 (7th Cir.1901), 76.

[20] See note 6.

[21] L. Heng Gee, *The Default Rules Relating to Joint Ownership of Patents Pitfallss for the Unwary*, in *Pertanika Journal Social Sciences & Humanities*, vol. 22, 2014, p. 57.

> of the thing patented, he can only grant that which he has himself […], namely, the right to sell or use thing patented»[22].

Moreover, this orientation is in line with the original sensitivity that founded the discipline of intellectual property in the United States. For example, James Madison, in 1788, two years before the promulgation of the Patent Act (1790), wrote about patents that «the public good fully coincides […] with the claims of individuals»[23].

At this point, we need to understand whether the U.S. default rules favor the licensing of joint patents. After all, from a green perspective, licensing enhances the potential of eco-sustainable patents: it spreads useful products to reduce pollution and stimulates further progress in the field. From this perspective, the U.S. system certainly gives greater freedom to each co-owner regarding licensing compared to veto-power systems. Indeed, the latter lead to the tragedy of the anticommons: each co-owner hinders the others from licensing the jointly patented technology, causing its underuse[24]. In this sense, Heller appropriately wrote:

> «Usually, private ownership creates wealth. But too much ownership has the opposite effect – it leads to resource underuse […]. If too many owners control a single resource, cooperation breaks down, wealth disappears, and everybody loses.
>
> There has been an unnoticed revolution in how we create wealth. In the old economy, twenty or thirty years ago, you invented a product and got a patent […]. Today, the leading edge of wealth creation requires assembly»[25].

At the same time, however, the U.S. model raises questions. Since each co-owner can grant to any licensor the joint patent, which is a common

[22] *Dunham v. Indianapolis & St. Louis R.R. CO.*, 8 F. Cas. 44 (N.D. III. 1876).

[23] J. Madison, *The Federalist Papers*, n. 43, 1788.

[24] «As effective as these tactics may be, however, they also present ethical dilemmas because although it may protect a firm's current position in their industry, it does so at the possible expense of pursuing environmental innovations in more far-flung technological domains». D. I. Leyva-De La Hiz et al., *Innovating for Good in Opportunistics Contexts: The Case for Firms' Environmental Divergence*, in *Journal of Business Ethics*, vol. 176, 2022, p. 706.

[25] M. Heller, *The Tragedy of the Anticommons: A Concise Introduction and Lexicon*, The Modern Law Review, vol. 6, 2013, p. 7. See also A. Fosfuri et al., *Shared Ownership of Intangible Property Rights: The Case of Patent Coassingments*, in *Journal of Legal Studies*, vol. 46, n. 2, 2017, p. 354.

property vulnerable to the tragedy of the commons: each co-owner, to maximize his profit, tends to grant the patent to more licensors than would happen if all co-owners decided on the licence[26]. In short, compared to veto-power systems, in the United States there is no risk of underuse of the joint patent, but rather the risk of overuse. Thus, the competition in the market increases and the potential profits for each co-owner are reduced, leading to an inexorable escape from joint patent development[27].

3. *How to encourage the creation of joint patents in the U.S.?*

On closer inspection, compared to veto-power systems, the intense freedom provided by the U.S. default rules in the non-exclusive licensing of jointly developed patents to third parties produces positive effects for the circulation of eco-sustainable inventions. Effectively, some studies demonstrate that in veto-power systems there is a propensity towards underuse of greater intensity compared to the inclination towards overuse in the tragedy of the commons. To understand the foundations of this assertion, it appears interesting this critical reading:

> «Clearly, there are important behavioral effects when anticommons property entitlements are created. Anticommons owners have a right to exclude others and a right to veto any transformation of the common resource. The prerogatives of an anticommons owner are perceived as something that they "own", and psychological attitudes are triggered for the protection of such entitlement. No sense of "harm" is associated with one's exercise of the property right, even though others may suffer a possible economic prejudice. Commons users instead do not perceive their opportunity to use the commons as something that they own. When overexploiting a common resource, they fully realize that they are imposing an economic prejudice to others and partially restrain from such abusive behavior»[28].

[26] See R. P. Merges; L. A. Locke, *Co-Ownership of Patents: a Comparative and Economic View,* in *Journal of the Patent and Trademark Office Society*, vol. 72, 1990, p. 592.

[27] See T. Hashimoto et al., *Managing joint R&D: an investigation into joint patent applications in Japan, US and Europe*, in *International Journal of Technology Transfer and Commercialisation*, vol. 11, n. 3, 2012, p. 154.

[28] S. Vanneste et al., *From "Tragedy" to "Disaster": Welfare Effects of Commons and Anticommons Dilemmas*, in *International Review of Law and Economics*, vol. 26, 2006, p. 117.

However, the problem of the tragedy of the commons remains in the U.S. model of default rules and therefore it is worth imagining possible solutions.

In this regard, a starting point could be the reflection of William Callyhan Robinson, an American academic and judge who became famous for his three-volume work *Law of Patents for Useful Inventions*, published in 1890, as well as for founding the Columbus School of Law in Washington. He was the first to critically observe the different discipline that distinguishes the co-ownership of a joint patent from other types of co-ownership. More specifically, he noted that in co-ownership situations outside patent law there are mutual obligations that induce the co-owners to restrain each other from excessive use. In particular, he connected the joint patent issue with the common of pasture rights, to highlight how in the latter there are some jurisprudential limits to the exploitation that are inexplicably not foreseen in the joint-patent co-ownership. Thus, he wrote:

> «Although no exact similitude exists between a patent privilege and any other property, yet the resemblance which it bears to a common of pasture is sufficient to suggest a possible solution of the present question. Both the patent privilege and the common of pasture are to be exercised within definite territory by specified means of enjoyment, and with a limited and determinable amount of profit. In both, the appropriation to himself, by one owner of more than his just share of such profit is an unjust invasion of the rights of the others, whether, in the one case, by the introduction of an excessive number of commonable beasts, or, in the other, by distributing the patent privilege to an increased number of […] licensees […]. Now the law finds no difficulty in regulating the rights and duties of commoners of pasture»[29].

Copyright law is another important area in which the U.S. legal system provides mutual limits between co-owners, especially as regards non-exclusive licensing. In copyright law, under Section 101 of Title 17 of the U.S. Code, a joint work is the result of the inseparable contributions of two or more authors. In the absence of a contrary agreement, they share equal and undivided ownership of the joint work. Each co-owner cannot proceed unilaterally to grant an exclusive license to third parties, but it is allowed to grant a non-exclusive license to use the entire work. However, unlike patent law, this possibility is subject to the duty to pay the other co-owners their

[29] W. C. Robinson, *The Law of Patents for Useful Inventions*, Little Brown & Co., Boston 1890, p. 571.

pro-rata shares of the related profit[30].

This rule on copyright law has a jurisprudential origin and demonstrates greater flexibility in the protection of private property than patent law. Moreover, copyright law has been characterized by many experiences, such as open innovation and fair use, which undermined the exclusive idea of property. Instead, patent law is still linked to a strong protection of individual privileges. In this sense, the controversy *Blackledge v. Weir & Craig Mfg. Co.* (1901)[31] is emblematic, since, for the first time expressly, the federal judges addressed the issue of sharing profits in matters of joint patents. In this case, the judges excluded the mandatory division of profits arising from the use of the joint patent, arguing that the exploitation of the same by a co-owner does not prejudice the rights of the other co-owners. This logic was also extended to profits from joint patent licensing. Indeed, the ruling states:

> «Use of the invention in any lawful way is not an appropriation of anything which belongs to another. The separate rights of the other owners remain unaffected. They are equally free to use the invention in all legitimate ways for their individual profits. Each is entitled to the fruits of his endeavors, taking no risk and expecting no reward from enterprises in which he does not choose to join. There is, therefore, no ground for the distinction instead upon between profits derived directly from the manufacture, use and sale of the patented article by the owner and profit derived by him from the sales of licenses»[32].

However, in subsequent cases there were judges who were skeptical about the appropriateness of this system. In the decision of *Talbot v. Quaker-State Oil Refining Co.* (1939), for example, it is written:

> «Each joint owner is in a very real sense at the mercy of any other. Each of them may use or license to others to use the invention with-

[30] «A co-owner of copyright must account to other co-owners for any profits he earns from licensing or use the copyright, […] but the duty to account does not derive from the copyright law's proscription of infringement. Rather, it comes from "equitable doctrines relating to unjust enrichment and general principles of law governing the rights of co-owners" (*Harrington v. Mure*, 186 F. Supp. 655, 657-658. S.D.N.Y. 1960)».*Oddo v. Reis*, MME, 743 F. 2d 630, 633 (9th Cir. 1984). «Each hav[e] an independent right to use or license the copyright, subject only to a duty to account to the other co-owner for any profits earned thereby». *Community for Creative Non-Violence v. Reid* F.2d 1485, 1489 (D.C. Cir. 1988). See also *Goodman v. Lee*, 78 F.3d 1007,1012 (5th Cir. 1996).

[31] *Blackledge v. Weir & Craig Mfg. Co.* (1901), 108 F. 71 (7th Circ.).

[32] *Blackledge v. Weir & Craig Mfg. Co.* (1901), 108 F. 71 (7th Circ.), p. 77.

> out the consent of his fellows, and without responsibility to such fellows for the profit arising from such use or license. This unlimited right to license other may, for all practical purposes, destroy the monopoly and so amount to an appropriation of the whole value of the patent»[33].

Given this skepticism, it cannot be excluded that the judges intend to reconsider this issue, perhaps also making use of comparative law. In this regard, the provision of a duty to account to the other co-owners for the granting of a non-exclusive license, as seen above, exists in China and France. Particularly, in France, in the absence of an agreement between the parties, the judge determines the amount of compensation *équitablement* to other co-owners «who do not personally exploit the invention or who have not granted a licence to exploit it»[34].This could be an interesting starting point for the U.S. common law, which is strongly permeated by case law solutions based on reasonableness and fairness. In this regard, this analysis of the French model it is noteworthy:

> «The determination of compensation will embarrass judges who, under the law, have no other instrument than *équité*. It emerges, however, from the preparatory work that the notion of *indemnité équitable* will have to consider what is attributable to the efforts of the exploiter. Everything that he personally directed to facilitate and increase the yield of the patent should not benefit those who remained passive and who did not show any interest in exploitation.
>
> […] It should be recognized that the compensation system risks threatening the objective of the law by blocking the exploitation of the patent: the co-owner who wishes to exploit the patent will perhaps hesitate in the face of an indemnity whose amount he cannot know in advance. But the legitimate interests of those who are not in a position to exploit cannot be totally sacrificed in the face of concerns for efficiency» [our translation][35].

In conclusion, the full freedom to grant non-exclusive licenses, provided

[33] *Talbot v. Quaker-State Oil Refining Co.* (1939), 104 F. 2d 967 (3rd Circ.), p. 968.

[34] <https://french-business-law.com/french-legislation-art/article-l613-29-of-the-french-intellectual-property-code/>.

[35] M. A. Perot Morel, *La réforme de la copropriété des brevets d'invention par la loi du 13 juillet 1978*, SJ/G-I-13, 1981, note 39, p. 10. For further information see also P. Lauzon, *Le partage des profits entre copropriétaires de brevets: Un survol international - Une réponse pour le Québec?*, in *Les Cahiers de propriété intellectuelle*, vol. 21, 2009, pp. 144-147.

by the U.S. default rules, certainly offers companies a reason to collaborate with each other to create joint patents, even if the risk of the tragedy of the commons could subsequently harm them. In the future, to overcome this issue, the federal judges could find a valid solution in the provision of a duty of accountability towards the other co-owners, similar to copyright.

This change would be useful not only to preserve monopoly right in patent collaborations, but also from a green perspective: all co-owners of the eco-sustainable joint patent would benefit from the licenses granted by the individual, the escape from joint patents would be reduced and the granting of licenses would concretely and on a large scale favor the exploitation of the benefits of the eco-sustainable joint patent.

Pierre-Emmanuel Rodriguez*

German Legal dogmatics and its contribution to the "scientificity" of law. An epistemological analysis of a law creation and application process

1. *Introduction*

« *The fact that dogmatic can be a legal science does not mean that the legal science is merely dogmatic* »[1]

The question of the "scientificity" of law is neither new nor outdated. Philosophers and legal theorists from all over the world have long pondered this issue. Several theories have been defended over time, but none has ever managed to win the consensus of the scientific community. In Germany, these discussions have taken a distinctive turn with the development of legal dogmatics, which has not yet been given the light it deserves.

German Legal dogmatics refers to the law creation and application process that has traditionally been at work in Germany, particularly since the end of the 19th century[2]. Legal dogmatics is defined as "a

* Pierre-Emmanuel Rodriguez earned his PhD at University of Reims Champagne-Ardenne and Paris Nanterre.

[1] I. Ausberg, "Lob der Dogmatik", *Rescriptum*, 2012, p. 66 : "Dass Dogmatik Rechtswissenschaf sein kann, trägt nicht den Umkehrschluss, Rechtswissenschaf sei nur Dogmatik".

[2] The first instance of "dogmatic" in German literature is to be found in the title of the journal "Jahrbücher für Dogmatik des heutigen römischen und deutschen Rechts", first published in 1857 by Rudolf von Jhering. Voir O. Jouanjan, *Une histoire de la pensée juridique en Allemagne (1800-1918). Idéalisme et conceptualisme chez les juristes allemands du XIXe siècle*, Paris, PUF, 2005, 364 p.

systematization of the law with a view to its application"[3]. It forms a bridge between practice and theory, providing a better understanding of positive law[4]. Legal dogmatics is also known for having several functions: a decision-making function (*Entscheigungsfunktion*), a law-development function (*Entwicklungsfunktion*) and a law-knowledge function (*Erkenntnisfunktion*)[5].

Legal dogmatics should not be confused with "legal reasoning" (*juristische Argumentation*)[6]. This last expression is the subject of various definitions, whose content depends on the authors and the country in which the reflections on the subject take place[7]. In a narrow way, it is mostly described as the "the judge's reasoning, as expressed in a judgment or ruling that provides the grounds for a legal decision"[8]. In a wider way, legal reasoning refers to the intellectual process that leads a jurist to methodically analyze a factual situation to identify a legal problem and provide a reasoned response. This includes not only the legal reasoning of judges, but also that of lawyers or professors[9].

For its part, German Legal dogmatics appears more precisely to be a system of propositions that make it possible to understand the law in force conceptually and systematically to guide its application[10]. If German legal

[3] M. Morlok, *Was heißt und zum welchen Ende studiert man die Verfassungstheorie*, 1988, Berlin, Duncker & Humblot, p. 40 et p. 43. On the meaning of legal dogmatic, see especially L. Häsemeyer, « Die Bedeutung der Rechtsdogmatik », *in* P. A. Windel, *German Legal Dogmatics. Beiträge zum internationalen Rechtsdialog*, Baden-Baden, Nomos, 2020, pp. 265-282.

[4] J. Harenburg, *Die Rechtsdogmatik zwischen Wissenschaft und Praxis*, Frankfurt am Main, Vico Verlag und Antiquariat Dr. Otto, 1986, p. 63 et s.

[5] J. Kersten, "Warum Dogmatik?", *Rescriptum*, 2012, pp. 67-69. For further details, see R. Stürner, "Das Zivilrecht der Moderne und die Bedeutung der Rechtsdogmatik", *JZ*, vol. 67, no. 1, 2012, pp. 10-24.

[6] W. Krawietz, R. Alexy, *Metatheorie juristischer Argumentation*, Berlin, Duncker & Humblot, 1984, 252 p.

[7] This plurality of definitions is well depicted in P. Brunet, "Le raisonnement juridique : une pratique spécifique ? », *International Journal for the Semiotics of Law*, 2013, pp. 1-15.

[8] For an example of the narrow definition of the legal reasoning, see C. Perelman, « Le raisonnement juridique », *Les Études philosophiques*, vol. 20, n°2, 1965, p. 133 : « le raisonnement du juge, tel qu'il se manifeste dans un jugement ou un arrêt qui motive une décision ».

[9] For a wider definition of legal reasoning by a French author, see J.-P. Tricoit, « Le raisonnement juridique », *in* J.-P. Tricoit, *Fiches de Culture juridique*, Paris, Ellipses, p. 207. In the same way, for an German author, see E. J. Lampe, « Problemanalyse als Grundlage der juristischen Argumentation (Juristische Aporetik) », *in Le raisonnement juridique : Actes du Congrès mondial de philosophie du droit et de philosophie sociale*, 1971, pp. 71-76.

[10] Generally presented as a characteristic of German legal science and culture, legal dogmatics is being developed in many foreign states. See for example about a French Legal dogmatics, Th. Hochmann, "Droits fondamentaux", in A. Gaillet, Th.

dogmatics can be described as a part of German legal reasoning, it must be distinguished from it by the specificity and precision of its functions. Especially its law-knowledge function must be taken into consideration when considering the contribution of legal dogmatics to the scientificity of law[11].

The idea of the scientificity of law presume the existence of a legal science. This idea has been, and still is, the subject of controversy[12]. Without going into the details of these discussions, it is simply possible to refet to the distinction between law and legal science as it is generally portrayed in the literature. Whereas law is made up of prescriptions, of legal norms that prohibit or authorize; legal science is a description of these prescriptions[13]. Legal science has no normative vocation: it is not concerned with the production of law, but only with the knowledge of law[14]. That's why the legal propositions formulated by legal science are either true or false, while legal prescriptions are either valid or not[15]. To find out whether legal dogmatics contributes to the scientificity of the law, it is necessary to carry out an epistemological analysis[16].

Hochmann, N. Marsch, Y. Vilain, M. Wendel (dir.), *Droits constitutionnels français et allemand. Perspective comparée*, 1ère, Issy-les-Moulineaux, LGDJ, 2019, pp. 365-368.

[11] In the same way, some authors refer to a "specific knowledge function" (spezifischen Erkenntnisfunktion), see M. Holoubek, "Bauelemente eines grundrechtsdogmatischen Argumentationsschemas: Schutzbereich - Eingriff - Schranken", *in* C. Grabenwarter, *Allgemeineheit der Grundrechte und Vielfalt gesellschaft*, Richard Boorberg Verlag, 1994, p. 64.

[12] The idea of the existence of a legal science is the subject of numerous controversies. Pessimists as to the existence of a legal science, see especially M. Troper, *La philosophie du droit*, 7e, Paris, PUF, 2024, 126 p. See also O. Leclerc, "Jalons prospectifs sur l'existence de reproductibilité dans la recherche juridique", *in* P. Deumier, O. Gout, D. Hiez, I. Maria, A. Prüm, (ed.), *Mélanges en l'honneur de Pascal Ancel*, Belgique, Larcier, 2021, pp. 175-186; F. Rouvière, "Le droit est-il une science si ses résultats ne sont pas reproductibles?", *RTDCiv*, n°3, 2021, p. 177.

[13] Kelsen drew a distinction between legal norms (*Rechtsnormen*) and legal propositions (*Rechtssätze*) formulated by legal science, see H. Kelsen, *Théorie pure du droit*, Paris, Bruylant - LGDJ, 1999, par. 16, pp. 78-82.

[14] In the same way, for a classic presentation of the distinction between legal science and law, see J. Chevallier, "Doctrine juridique et science juridique", *Droit et Société : Revue internationale de théorie du droit et de sociologie juridique*, 2002, pp. 103-119.

[15] Legal science can simply be seen as a description of legal phenomenon. Unlike legal dogmatics, legal science is not involved in the creation of law. M. Troper, "Entre science et dogmatique, la voie étroite de la neutralité", *Théorie du droit et science*, Paris, PUF, 1994.

[16] As Le Moigne sums up, "an epistemological approach leads us to ask three questions: a gnoseological question - what is knowledge? what is there to know? -a methodological question - how is knowledge constituted? - an axiological question - how do we assess the value or validity of the knowledge produced?, see J.-L. Le Moigne, *Les épistémologies constructivistes*, Que sais-je?, PUF, 2007, p. 6.

Epistemology is "the study of the formation and development of legal knowledge"[17]. More precisely, epistemology is "an analytical and critical reflection on the development of scientific legal knowledge and of the methods used to justify and validate this knowledge"[18]. It is important to precise that the epistemological analysis of German legal dogmatics is not focused on the concepts and rules generated by dogmatics. Rather, it is concerned with legal dogmatics itself, as a law-understanding tool.

This contribution therefore aims to answer the question of whether German legal dogmatics contributes to the scientificity of the law.

Without any doubt does legal dogmatics contribute to the scientificity of law by making it possible to reproduce its results and verify their accuracy. However, the characteristics of legal dogmatics can undermine its contribution to the scientificity of the law, by giving rise to a flawed or erroneous understanding of positive law. It is therefore appropriate to consider in turn the content (I) and the condition (II) of the contribution of legal dogmatics to the scientificity of the law.

2. *The content of legal dogmatics contribution to the scientificity of law*

Those who deny the scientificity of law, or the existence of a legal science, argue that the law produces results that are not reproducible or not empirically verifiable[19]. The reproducibility of a result and the possibility of falsifying it - i.e. refuting it through empirical observations - is a condition

[17] See C. Atias, *Science des légistes, savoir des juristes*, 3e, Aix-en-Provence, Presses universitaires d'Aix-Marseille, 1993, p. 33. Epistemology is also described as "an analytical and critical reflection on the sciences", see J.-M. Berthelot (ed.), *L'épistémologie des sciences sociales*, Quadrige, PUF, 2012, p. 14. In the same way, epistemology is "knowledge of the conditions of scientific production", see M. Miaille, *Une introduction critique au droit*, François Maspero, 1976, p. 35.

[18] A. Geslin, « L'importance de l'épistémologie pour la recherche en droit », *in* B. Sergues (ed.), *La recherche juridique vue par ses propres acteurs*, Toulouse, Presses de l'Université de Toulouse Capitole, 2018, pp. 79-130.

[19] On reproducibility as a criterion of scientificity, see recently O. Leclerc, "Jalons prospectifs sur l'exigence de reproductibilité dans la recherche juridique", *in* P. Deumier, O. Gout, D. Hiez, I. Maria , A. Prüm (ed.), *Mélanges en l'honneur de Pascal Ancel*, Paris, Larcier, 2021, p. 177 et seq.; P. Jestaz, "Qu'est-ce qu'un résultat en droit?", *in* J.- L. Bergel, A. Bénabent (ed.), *Mélanges Philippe Malinvaud*, Paris, LexisNexis, 2014, p. 293 et seq.; F. Rouvière, "Le droit est-il une science si ses résultats ne sont pas reproductibles?", *RTD Civ.*, n°3, 2021, p. 747 et seq.

of scientificity that law lacks[20]. German legal dogmatics does, however, provide an answer to this problem, and this is precisely where resides its contribution to the scientificity of law. Legal dogmatics makes it possible to verify - or falsify - the law as applied by the courts (A) and as presented in the scholarly studies in literature (B).

2.1 *The verifiability of jurisprudential solutions through the lens of legal dogmatics*

The systematic dimension of legal dogmatics makes it possible to verify the law as applied by the courts. Especially, it makes it possible to check that the decision-making process and the outcome of a court decision are in line with dogmatic solutions.

In Germany, disputes resolution is based on argumentation and review schemes (*Argumentations- und Fallprüfungsschema*), whose solutions have long been tried and tested[21]. This approach ensures that disputes are not resolved differently each time, but according to a detailed method, using specific legal criteria and in line with pre-established solutions[22]. In litigation, judges do not deviate from the dogmatic analysis framework and its solutions, because they know that their decision would be overturned by the higher court. Legal dogmatics thus contributes to the harmonization of the law applied by the courts, the transparency of the decision-making process and the legitimacy of court decisions.

The most famous illustration of the verifiability of legal decisions can be found in the traditional control of infringements of fundamental rights. Following German fundamental rights dogmatics, the judge must carry out a three-stage review[23]. First, it must verify that the restricted human

[20] According to Karl Popper's famous criterion, what can be falsified is scientific, see K. Popper, *La logique de la découverte scientifique*, Paris, Payot, 1973, p. 23 et seq. Legal dogmatics could be the "functional equivalent" of the Popperian test of falsifiability sought by certain french authors, see especially F. Rouvière, "Karl Popper chez les juristes : peut-on falsifier un concept juridique ?", *RRJ - Droit prospectif*, 2015, pp. 2213-2230.

[21] All German legal handbooks contain such schemas, see e.g. T. Kingreen, R. Poscher, *Grundrechte, Staatsrecht II*, 40e, Heidelberg, C.F. Müller, 2024, 420 pp.

[22] For further details, see Th. Hochmann, "Droits fondamentaux", *in* A. Gaillet, Th. Hochmann, N. Marsch, Y. Vilain, M. Wendel (ed.), *Droits constitutionnels français et allemand. Perspective comparée*, 1ère, Issy-les-Moulineaux, LGDJ, 2019, p. 365.

[23] This analytical framework, which is still in force today, was the subject of considerable doctrinal controversy in the early 2000s, see in particular PAPIER (H.-J.), "Aktuelle grundrechtsdogmatische Entwicklungen in der Rechtsprechung des

behavior falls within the scope (*Schutzbereich*) of one of the fundamental rights invoked by the claimant[24]. Then, it must verify that the disputed state measure does indeed constitute an infringement (*Eingriff*) of this fundamental right[25]. Lastly, the judge must carry out a proportionality check to ensure that the infringement of the fundamental right is justified (*Eingriffsrechtsfertigung*)[26]. This last stage has been criticized because of the discretionary latitude conferred on the judge by the proportionality test[27]. However, the judge must justify each of these steps. In this way, it is possible to verify the accuracy not only of the result of the review - i.e. the outcome given to the dispute - but also of the process used by the judge to get to a solution in a specific case[28].

Bundesverfassungsgerichts. Schutzbereich - Eingriff - Gesetzvorhebalt", *in* D. Merten, H.-J. Papier (ed.), *Grundsatzfragen der Grundrechtsdogmatik*, Heidelberg, C.F. Müller, 2007, pp. 81-99; E.-W. Böckenförde, "Schutzbereich, Eingriff, verfassungsimmanente Schranken, Zur Kritik gegenwärtiger Grundrechtsdogmatik", *Der Staat*, vol. 42, no. 2, 2003, pp. 165-192. The controversy focused especially on the first of the three examination stages. See the discussions between Professors Kahl and Hoffmann-Riem, W. Hoffmann-Riem, "Enge oder weite Gewährleistungsgehalte der Grundrechte?", *in* M. Bäuerle, A. Hanebeck, C. Hausotter, M. Mayer, J. Mohr, M. Mors, K. Preedy, A. Wallrabenstein (ed.), *Haben wir wirklich Recht? - Zum Verhältnis von Recht und Wirklichkeit. Beiträge zum Kolloquium anlässlich des 60. Geburtstags von Brun-Otto Bryde*, Baden-Baden, Nomos, 2003, pp. 53-76; W. Kahl, "Vom weiten Schutzbereich zum engen Gewährleistungsgehalt", *Der Staat*, vol. 43, n°2, 2004, pp. 167-202; W. Hoffmann-Riem, "Grundrechtsanwendung unter Rationalitätsanspruch. Eine Erwiderung auf Kahls Kritik an neueren Ansätzen in der Grundrechtsdogmatik", *Der Staat*, vol. 43, no. 2, 2004, pp. 203-234.

[24] On the question of the scope of fundamental rights, see D. Merten, "Grundrechtlicher Schutzbereich", *in* D. Merten, H.-J. Papier (ed.), *Handbuch der Grundrechte in Deutschland und Europa. Band III, Grundrechte in Deutschland: allgemeine Lehren II*, Heidelberg, C. F. Müller, 2009, pp. 3-85; U. J. Schröder, "Der Schutzbereich der Grundrechte", *JA*, vol. 48, n°9, 2016, pp. 641-648.

[25] On the dogmatic concept of infringement and the evolution of its legal criteria, see M. Holoubek, "Der Grundrechtseingriff - Überlegungen zu einer grundrechtsdogmatischen Figur im Wandel", *in* D. Merten, H.-J. Papier (ed.), Grundsatzfragen der Grundrechtsdogmatik, Heidelberg, C.F. Müller, 2007, pp. 17-34.

[26] Proportionality control ultimately involves the judge weighing up (*Abwägung*) the conflicting interests at stake in the dispute, see H. Stück, "Subsumption und Abwägung", *ARSP*, vol. 84, no. 3, 1998, pp. 405-419; J. Rückert, "Abwägung - die juristische Karriere eines unjuristischen Begriffs oder: Normenstrenge und Abwägung im Funktionswandel", *JZ*, vol. 66, no. 19, 2011, pp. 913-923.

[27] W. Leisner, *Der Abwägungsstaat. Verhältnismäßigkeit als Gerechtigkeit ?*, Berlin, Duncker & Humblot, 1997, 251 p. ; K.-H. Ladeur, *Kritik der Abwägung in der Grundrechtsdogmatik*, Tübingen, Mohr Siebeck, 2004, 83; J.-R. Siekmann, "Autonome Abwägung", *ARSP*, vol. 90, n°1, 2004, pp. 66-85.

[28] Legal dogmatics has a memory function (*Speicherfunktion*) because it constitutes

2.2 *The verifiability of scholarly studies through the lens of legal dogmatics*

The systematic dimension of legal dogmatics also makes it possible to verify the consistency of scholarly studies. By analyzing scholarly studies in the light of legal dogmatics, it is possible to reproduce their results and thus ensure their scientificity.

In Germany, a scholarly study is considered as a scientific study if it follows the legal dogmatics requirements. Authors must adopt a specific reasoning process, structured in three stages, to ensure the reproducibility and therefore the verifiability of their studies[29]. The first step in this process involves the decontextualization of the jurisprudential solution which is the subject of a doctrinal study. For its author, the aim is to detach himself from the concrete circumstances of the dispute to identify the particularities of the jurisprudential solution studied. The second step involves increasing generality. The aim is to develop abstract considerations based on the jurisprudential solution, to make it possible to extend its application to a group of cases which are similar to the original dispute. For the author, this involves constructing "figures, schemes and concepts" (*Figuren, Schemata, Konzepten*) to form resolution models for future cases (*künfige Fallgestaltungen Schablonen*)[30]. Finally, the third and last stage, known as "recontextualization", involves testing the functionality of the systematization by mobilizing it to solve concrete cases. This final step ensures that the created system is operational and therefore relevant[31].

The dogmatic requirements of this legal reasoning process are a guarantee of the scientificity of German scholarly studies, as they enable anyone to reproduce their stages and verify their results[32]. When a scholarly study

a bank of solutions that judges must apply in a specific case, depending on the characteristics of the dispute. In the same way, see C. Bumke, "Publikumsinformation. Erscheinungsformen und verfassungsrechtlicher Rahmen einer Handlungsform des Gewährleistungsstaates", *Die Verwaltung*, n°37, 2004, p. 33.

[29] For some authors, this process only consists of two stages: the first one involving decontextualization and generalization, and the second one, known as "re-specification" (*Respezifzierung*), which corresponds to the systematic application to concrete cases. See I. Ausberg, "Lob der Dogmatik", *Rescriptum*, 2012, pp. 63-66.

[30] See I. Ausberg, "Lob der Dogmatik", *Rescriptum*, 2012, p. 63.

[31] Legal dogmatics "puts in order and deepens the legal rules enacted, so as to present them systematically and shed light on their potential applications", see P. Amselek, "Propos introductifs", *in* P. Amselek (ed.), *Théorie du droit et science*, Paris, PUF, 1994, pp. 10-11.

[32] The three stages of legal reasoning according to dogmatic logic never appear so clearly in scholarly studies. However, it is possible to find their content systematically, as this structure of legal reasoning is both a criterion of scientificity and an academic

ignores one of the dogmatic reasoning stages, this may mean that the system that has been created is not functional[33]. However, the scientificity of a scholarly study cannot be presumed simply because it includes the three stages of the dogmatic reasoning process. It is crucial to check that each stage of the reasoning process follows a logical sequence, and to verify that the system created contains no mistakes or gaps. So, in Germany, a particular attention is given to the respect of dogmatic requirements in legal research.

To sum it up, legal dogmatics contributes to the scientificity of law thanks to its systematic dimension, which makes it possible to verify the law as applied by the courts and as presented by scholarly studies. In this way, legal dogmatics guarantees a logical and rational understanding of positive law. However, care must be taken to ensure that the characteristics of legal dogmatics do not reduce or overshadow its contribution to the scientificity of law. This is the second part of my presentation which deals with the condition of legal dogmatics contribution to the scientificity of law.

3. *The condition of legal dogmatics contribution to the scientificity of law*

While legal dogmatics is a criterion of scientificity and a tool for understanding positive law, its ideological impregnation may lead to a misunderstanding of legal norms and thus undermine its contribution to the scientificity of law (A). It is therefore important to promote a responsible use of legal dogmatics through an epistemological analysis that can reveal its underlying ideology and the values it disseminates (B). Here are the two ideas I'm now going to develop.

3.1 *The unavoidable ideological impregnation of legal dogmatics*

Legal dogmatics is known for its axiological neutrality[34]. It would be the

requirement for German jurists. See M. Jestaedt, "Phänomen Bundesverfassungsgericht. Was das Gericht zu dem macht, was es ist", *in* M. Jestaedt, O. Lepsius, C. Möllers, C. Schönberger (ed.), *Das entgrenzte Gericht - Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgerichts*, 3e, Berlin, Suhrkamp AG, 2019, p. 131.

[33] In the literature, the absence of one of these steps can earn the author of a study published in the literature significant criticism from his peers. See, for example, R. Alexy, "Jörn Ipsens Konstruktion der Grundrechte", *Der Staat*, vol. 52, n°1, 2013, pp. 87-98.

[34] See the presentation of legal dogmatics in the papers published before the entry into

result of a purely legal reflection oriented towards logic and rationality. Free of all extra-legal considerations, legal dogmatics would also be impartial, in line with the logic of positivism[35]. In this way, legal dogmatics would contribute to the scientificity of law.

However, time and experience have shown that legal dogmatics is not as neutral as its proponents would have us believe. The creation and application of law, in Germany as elsewhere, is influenced by ideologies. Especially, German legal dogmatics has an ideological impregnation that contributes to the dissemination of certain values[36]. Ignorance of the ideology that underlies German legal dogmatics can lead to a misunderstanding of the law, and thus compromise its contribution to the scientificity of law.

When the ideological impregnation of legal dogmatics is glossed over under the pretext of axiological neutrality, there is a serious risk for the dogmatic to being instrumentalized for dangerous purposes. For example, during the Second World War, legal dogmatics has been instrumentalized to justify anti-Semitic legislation[37]. In France, jurists exploited legal dogmatics to perpetuate and justify immoral regulations under what we called "le régime de Vichy". "The technicity of the discussion and the abstract formalism of the reasoning masked the concrete implications and dramatic consequences of the analyzed legislations"[38]. Legal dogmatics has thus been criticized for being disconnected from social and political reality[39].

force of the Basic Law. See, for example, P. Laband, Das Staatsrecht des Deutschen Reiches, Band I, 5e, Tübingen, J.C.B. Mohr, 1911-1914, p. 120; B. Windscheid, *Lehrbuch des Pandektenrechts*, Band I, 9e, Frankfurt am Main, Rütten & Loening, 1906, p. 110.

[35] For a general look at the pros and cons of a dogmatic approach, see C. Waldhoff, "Kritik und Lob der Dogmatik", *in* G. Kirchhof, S. Magen, K. Schneider (ed.), *Was weiß Dogmatik?*, Tübingen, Mohr Siebeck, 2012, pp. 17-38.

[36] As Professor Lochack notes, "legal dogmatics, under the guise of respecting the postulate of neutrality, contributes to disseminating the values underlying current legislation and reinforcing belief in their legitimacy", see D. Lochack, M. Troper, "La neutralité de la dogmatique juridique: mythe ou réalité?", *in* P. Amselek (ed.), *Théorie du droit et science*, Paris, PUF, 1994, p. 293.

[37] D. Lochak, "Le droit sous Vichy ou les mésaventures du positivisme", *in* Publications du CURAPP (ed.), *Les usages sociaux du droit*, Paris, PUF, 1989, pp. 252-285.

[38] D. Lochack, M. Troper, "La neutralité de la dogmatique juridique: mythe ou réalité?", *in* P. Amselek (ed.), *Théorie du droit et science*, Paris, PUF, 1994, pp. 293-324, see spec. p. 306: "a legitimization of anti-Semitic law by academic doctrine under the cloack of purely "technical" and objective studies".

[39] More generally, this is the criticism aimed at positivism, see A. Viala, « Le positivisme juridique : Kelsen et l'héritage kantien », *Revue interdisciplinaire d'études juridiques*, vol.

Nevertheless, an epistemological analysis reveals the values underlying legal dogmatics. In the German system, legal dogmatics is oriented towards the protection of human dignity as an intangible value of the German Basic Law[40]. Knowing this specific framework of thought enables us to grasp the orientation of the law creation and application process in Germany, and thus prevent any misunderstanding of the law. Therefore, it is necessary to understand this law process to prevent any false knowledge of positive law. This is why it is crucial to make a responsible use of legal dogmatics to preserve its contribution to the scientificity of law.

3.2 *For a responsible use of legal dogmatics*

Legal dogmatics can only contribute to the scientificity of law if it is used responsibly. Those who use it must remain aware of the historical and intellectual conditioning of legal dogmatics, so as not to lose sight of the ideology behind it and the values it disseminates. As Goethe wrote, jurists must not practice vulgar dogmatics (*Vulgärdogmatik*) by blindly and systematically applying so-called dogmatic solutions whose ideological backgrounds are ignored by those who apply it[41]. To avoid making this mistake, it is possible to combine usual dogmatics (*Gebrauchsdogmatik*) with scientific dogmatics (*Wissentschafliche Dogmatik*)[42].

Usual dogmatics is mainly applied by the courts. It refers to the systematized solving of disputes based on legal criteria, without any thought being given to the basis of these solutions[43]. This is what the scholarly literature refers to as the discharge and memory function (*Entslastungs- und Speicherfunktion*) of usual dogmatics, which aims to simplify and legitimize the judicial workload[44]. In the same way, usual dogmatics is also present at

67, n°2, 2011, pp. 95-117.

[40] For this reason, human dignity is enshrined in Article 1 of the German Basic Law, which states that "the dignity of the human being is intangible".

[41] See E. Trunz, *Goethes Werke. Band IX. Dichtung und Wahrheit*, 13e, Hamburg, C. Wegner, 1999, p. 360.

[42] On the distinction between usual dogmatics and scientific dogmatics, see R. Stürner, "Das Zivilrecht der Moderne und die Bedeutung der Rechtsdogmatik", *JZ*, vol. 67, n°1, 2012, pp. 10-24.

[43] W. Hassemer, "Dogmatik zwischen Wissenschaft und richterlicher Pragmatik: Einführende Bemerkungen", *in* G. Kirchhof, S. Magen, K. Schneider, *Was weiß Dogmatik?*, Tübingen, Mohr Siebeck, 2012, p. 14 et s.

[44] On the various functions of dogmatics, see R. Stürner, "Das Zivilrecht der Moderne und die Bedeutung der Rechtsdogmatik", *JZ*, vol. 67, n°1, 2012, pp. 10-24.

German universities[45]. It provides students with immediately operational legal tools. Nevertheless, the ideological foundations of these tools are mostly ignored by the students who apply it once they have finished their studies[46]. So, to avoid repeating past mistakes, we need to ensure that the usual dogmatics remains combined with scientific dogmatics.

The task of scientific dogmatics is to systematize positive law and evaluate court decisions[47]. In Germany, this scientific dogmatics is the result of a dialogue between law professors and judges[48]. Even if this cooperation has sometimes given rise to considerable controversy[49], it remains nonetheless essential, since it helps to avoid the legal positivism of the Federal Constitutional Court (*Bundesverfassungsgerichtspositivismus*)[50].

[45] For further details from a Franco-German perspective, see C. D. Classen, "Französisches Grundrechtsverständnis: kaum Dogmatik, objektiv-rechtliche Traditionen, subjektiv-rechtlichen Perspektiven?", *JöR*, vol 68, n°1, 2020, pp. 213-240.

[46] As early as the first year of law school, all German students learn, for example, that an infringement of fundamental rights is examined in three stages: scope - infringement - justification. The teaching of fundamental rights dogmatics at German universities, however, often omits the intellectual and historical basis of this review. As a result, many students apply this analytical scheme to solve practical cases, without even knowing why this method is the one chosen by the courts. On this point, see R. Van Gestel, H.-W. Micklitz, E. L. Rubin (ed.), *Rethinking legal scholarship: a transatlantic dialogue*, New York, Cambridge University Press, 2017, 543 p. See also the English translation of M.-J. Möllers, *Legal methods: how to work with legal arguments*, Oxford, Hart, 2020, 584 p., more precisely p. 306 et seq., p. 308.

[47] D. Grimm (ed.), Vorbereiter - Nachbereiter? Studien zum Verhältnis von Verfassungsrechtsprechung und Verfassungsrechtswissenschaft, Tübingen, Mohr Siebeck, 2019, 424 p.

[48] W. Hassemer, "Dogmatik zwischen Wissenschaft und richterlicher Pragmatik: Einführende Bemerkungen", *in* G. Kirchhof, S. Magen, K. Schneider, *Was weiß Dogmatik?*, Tübingen, Mohr Siebeck, 2012, pp. 3-16. Moreover, on average, half the members of Germany's Federal Constitutional Court are law professors, which facilitates the development of scientific dogmatics by creating a "common space for discussion" (gemeinsamen Kommunikationsraum) M. Jestaedt, "Phänomen Bundesverfassungsgericht. Was das Gericht zu dem macht, was es ist", *in* M. Jestaedt, O. Lepsius, C. Möllers, C. Schönberger (ed.), Das entgrenzte Gericht - Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgerichts, 3e, Berlin, Suhrkamp AG, 2019, p. 126.

[49] See, for example, B. Schlink, "Abschied von der Dogmatik. Verfassungsrechtsprechung und Verfassungsrechtswissenschaft im Wandel", *JZ*, n°4, 2007, pp. 157-162. In the early 2000s, some famous controversies occurred in the dogmatics of fundamental rights, see especially D. Murswiek, "Grundrechtsdogmatik und Wendepunkt?", *Der Staat*, vol. 45, n°4, 2006, pp. 473-500.

[50] B. Schlink, "Die Entthronung der Staatsrechtswissenschaft durch die Verfassungsgerichtsbarkeit", *Der Staat*, vol. 28, 1989, pp. 161-172.

The combination of usual dogmatics and scientific dogmatics also prevents any slide towards dogmatism (*Dogmatismus*), which means the crystallization of legal criteria and analytical frameworks. Scientific dogmatics ensures that usual dogmatics is adapted to new societal challenges[51].

4. *Conclusion*

German legal dogmatics is the guarantee of a law systematization that simplifies the understanding and thus the knowledge of positive law. Its systematic dimension makes it possible to check the accuracy of legal decisions and scholarly studies. This is how the legal dogmatics contribution to the scientificity of law can be summed up. However, legal dogmatics must always be used responsibly to ensure that this contribution is not limited or even totally compromised. Jurists must remain aware of the historical and intellectual conditioning of dogmatic solutions and analytical frameworks. At least, this is the requirement for legal dogmatics to contribute to the scientificity of law. As professor Kersten once said, "Only the one who is informed about legal history, legal theory or comparative law will also be a good legal dogmatician, which means that he will apply normative principles reflexively while developing them creatively"[52].

[51] Academic discussions within the framework of scientific dogmatics make it possible to "subject [the criteria of usual dogmatics] to a critical appreciation, highlighting their qualities but above all their imperfections (...), an appreciation which may lead to proposals for reform and improvement", see P. Amselek, "Propos introductifs", *in* P. Amselek (ed.), *Théorie du droit et science*, Paris, PUF, 1994, pp. 10-11.

[52] J. Kersten, « Warum Dogmatik ? », *Rescriptum*, 2012, p. 68 : « Nur wer rechtshistorisch, rechtstheoretisch bzw. rechtsvergleichend informiert ist, wird auch ein guter Rechtsdogmatiker sein, also normative Leitsätze reflektiert anwenden und zugleich auch kreativ weiterentwickeln ».

This volume originates from the second edition of the International Doctoral Workshop, organized in 2024 by the PhD candidates of the Law & Social Change program at Roma Tre University. The initiative offered young researchers from diverse academic backgrounds a space for open and collaborative dialogue on contemporary legal issues. The collected contributions explore how legal systems can respond to the challenges posed by technological innovation, climate change, and global social transformations. From the regulation of artificial intelligence and digital services to the implications of blockchain, media pluralism, international environmental law, and the theoretical foundations of legal reasoning, the volume presents a pluralistic and interdisciplinary perspective. Born from dialogue among early-career scholars and supported by the academic community of Roma Tre, the book reflects the vitality of emerging legal research and its ability to question traditional paradigms of law.

BEATRICE BICHI RUSPOLI FORTEGUERRI

is a PhD candidate in Law & Social Change at Roma Tre University. Her research focuses on the relationship between competition law and environmental sustainability within the European Union legal framework. She earned her law degree with honours from the University of Milan "Statale" and is qualified to practice law in Italy. She has gained experience at the Italian Competition Authority and the European Commission, focusing on issues related to energy, competition, and the environment.

FEDERICO BONITO

is a PhD Candidate in Law & Social Change at Roma Tre University, researching the use of general principles of law by International Administrative Tribunals. A legal trainee focusing on international legal disputes, including litigation before the European Court Human Rights litigation, he previously worked at the Legal Office of the NATO Joint Force Command in Naples, where he participated in the activities of the NATO Mission Appeals Tribunal (MAT). He holds a law degree with honours from Roma Tre University.

Roma Tre