Co-funded by
the European Union

EUROPEAN FUNDAMENTAL VALUES IN THE DIGITAL ERA

Editors:
Yulia Razmetaeva,
Nataliia Filatova-Bilous

Kharkiv
“Pravo”
2024

DOI: https://doi.org/10.31359/9786178518073
UDC 340+343+347+140
E91

European Fundamental Values in the Digital Era : [monograph] / eds.:
E91 Yulia Razmetaeva, Nataliia Filatova-Bilous ; European Union ; Jean Monnet Centre of Excellence "European Fundamental Values in Digital Era" ; Yaroslav Mudryi National Law University. – Kharkiv : Pravo, 2024. – 316 p. – DOI: https://doi.org/10.31359/9786178518073.

ISBN 978-617-8518-07-3

This monograph is the result of cooperation between Ukrainian and European researchers on European fundamental values in the digital age. The book consists of three parts, the first of which is devoted to the general theoretical analysis of European fundamental values, the second – to the way the European fundamental values are implemented in modern contract and tort law, and the third – to the implementation of European fundamental values in procedural law in the digital era.

The book will be interesting to scholars and practitioners, students and teachers, as well as anyone interested in law and digital technologies.

UDC 340+343+347+140

This publication is part of the Jean Monnet Centre of Excellence "European Fundamental Values in Digital Era", EFVDE (2022–2025), 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, Grant Agreement decision no 101085385, co-funded by the European Union. This collective monograph is open access publication.

ISBN 978-617-8518-07-3

ЄВРОПЕЙСЬКІ ФУНДАМЕНТАЛЬНІ ЦІННОСТІ В ЦИФРОВУ ЕРУ

Редакторки:
Юлія Размєтаєва,
Наталія Філатова-Білоус

Харків
«Право»
2024

DOI: https://doi.org/10.31359/9786178518073
УДК 340+343+347+140
Е91

Європейські фундаментальні цінності в цифрову еру : [монографія] / Е91 ред.: Юлія Размєтаєва, Наталія Філатова-Білоус ; Європ. Союз ; Центр Досконалості Жана Моне «Європ. фундамент. цінності в цифр. еру» ; Нац. юрид. ун-т ім. Ярослава Мудрого. – Харків : Право, 2024. – 316 с. – DOI: https://doi.org/10.31359/9786178518073. – (Англ. і укр. мовою).

ISBN 978-617-8518-07-3

Ця монографія є результатом співпраці українських та європейських учених у сфері дослідження європейських фундаментальних цінностей у цифрову епоху. Книга складається з трьох частин, перша з яких присвячена загальнотеоретичному аналізу європейських фундаментальних цінностей, друга – тому, як європейські фундаментальні цінності імплементовані в сучасному договірному й деліктному праві, а третя – імплементації європейських фундаментальних цінностей у процесуальне право в цифрову епоху.

Книга буде цікава для науковців та практиків, студентів і викладачів, а також усіх, хто цікавиться проблематикою права й цифрових технологій.

УДК 340+343+347+140

Ця публікація є частиною проєкту Центр Досконалості Жана Моне «Європейські фундаментальні цінності в цифрову еру», EFVDE (2022–2025), 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, грантова угода 101085385, що співфінансується Європейським Союзом. Ця колективна монографія є виданням у відкритому доступі.

Застереження:

ISBN 978-617-8518-07-3

CONTENTS / ЗМІСТ

Theme 2
Implementation of European fundamental values in contract and tort law
Тема 2
Імплементація європейських фундаментальних цінностей у договірному та деліктному праві

Theme 3
Procedural aspects of the implementation of European fundamental values in the digital era

Тема 3
Процесуальні аспекти імплементації фундаментальних європейських цінностей у цифрову еру

From editors

This book is a result of fruitful collaboration between experts from different spheres who spent many sleepless nights and burnt many candles at both ends. In it you will find a kaleidoscopic variety of approaches and perspectives including philosophical, legal, political, technological and futurological. It is composed of three parts: Theme 1 'The concept of European fundamental values in the digital era: rights, principles and data', Theme 2 'Implementation of European fundamental values in contract and tort law' and Theme 3 'Procedural aspects of the implementation of European fundamental values in the digital era'.

We are incredibly grateful to the authors of this book for the creativity, in-depth analysis, and enthusiasm which they manifested in their contributions.

In the Prologue written by *Stéphanie Laulhé Shaelou* you will find a more detailed guide to this book and the description of the projects that led to its emergence. Authors who contributed to Theme 1 focus on general issues concerning European fundamental values in the digital era. In the contribution prepared by *Yulia Razmetaeva* you will find a broad theoretical and philosophical analysis of factors challenging fundamental triad of human rights, democracy, and the rule of law in the digital age. *Gintarė Makauskaitė-Samuolė* in her contribution reviews existing approaches to transparency in the European digital ecosystem and explains the necessity to adjust transparency measures in the current digitalized realm. The chapter prepared by *Petro Sukhorolskyi* is dedicated to the study of values most often associated with the right to the protection of personal data in light of a new totalitarian threat which is fuelled by current digital trends. *Bohdan Karnaukh* in his contribution explores the right to be forgotten within the broader framework of privacy rights, focusing on seminal cases and legal developments in Europe.

Theme 2 focuses on the ways European fundamental values are implemented in contract and tort law in the digital age. It starts with the contribution prepared by *Nataliia Filatova-Bilous* analyzing modern trends of contract law and the possibility of horizontal application of the European fundamental values to contractual relationships in the digital era. The chapter prepared by *Oksana Kiriiak* presents an in-depth analysis of the multifaceted phenomenon of digital silence, examining its definition, manifestations, legal implications, societal dynamics and ethical considerations. In his contribution *Kyrylo Anisimov* analyzes national civil legislation and practice regarding the form of a transaction, signature and, to some extent, the procedure for concluding a contract and the way it recognizes modern trends and challenges brought about by digitalization.

Theme 3 is dedicated to the implementation of European fundamental values into the procedural law in the digital age. It starts with the contribution prepared by *Nataliia Sakara* focusing on the observance of the right to a fair trial when information technologies are employed in civil proceedings. *Tetiana Tsuvina* in her contribution examines the potential applications of ChatGPT in legal proceedings, with a particular focus on its use by litigants and their attorneys in the preparation of procedural documents. In their chapter *Oksana Kaplina and Iryna Krytska* identify the main vectors of digital transformation of criminal procedure and analyze them with due regard to the possible benefits of digital technologies in criminal proceedings and the potential risks which they may pose.

It is an as open-access book published within the project of the Jean Monnet Centre of Excellence “European Fundamental Values in Digital Era”, EFVDE (2022–2025), 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, Grant Agreement decision no 101085385, co-funded by the European Union.

We hope you enjoy delving with us into the exploration of European fundamental values in the digital era. We welcome any feedback and invite each and every one of you into a discussion of what future awaits the humanity.

Yulia Razmetaeva and Nataliia Filatova-Bilous

Від редакторок

Ця книга – результат плідної співпраці фахівців з різних сфер, які провели багато безсонних ночей і спалили багато свічок, працюючи над нею. У ній ви знайдете калейдоскопічне розмаїття підходів і точок зору, включаючи філософські, правові, політичні, технологічні та футурологічні. Вона складається з трьох частин: Тема 1 "Концепція європейських фундаментальних цінностей у цифрову еру: права, принципи та дані", Тема 2 "Імплементація європейських фундаментальних цінностей у договірному та деліктному праві" та Тема 3 "Процесуальні аспекти імплементації фундаментальних європейських цінностей у цифрову еру".

Ми неймовірно вдячні авторам цієї книги за творчий підхід, глибокий аналіз та ентузіазм, які вони проявили у своїх роботах.

У Пролозі від *Стефані Лаулє Шелоу* ви знайдете більш детальну інформацію про цю книгу та про проєкти, які допомогли їй з'явитися. Автори, які підготували розділи до Теми 1, зосереджуються у своїх роботах на загальних питаннях, що стосуються європейських фундаментальних цінностей в цифрову епоху. У розділі *Юлії Размєтаєвої* ви знайдете широкий теоретико-філософський аналіз факторів, що кидають виклик фундаментальній тріаді прав людини, демократії та верховенства права в цифрову епоху. *Гінтаре Макаускайте-Самуоле* у своєму розділі розглядає наявні підходи до концепції прозорості в європейській цифровій екосистемі та пояснює необхідність адаптації механізмів, що забезпечують прозорість у сучасній цифровій сфері. Розділ, підготовлений *Петром Сухорольським*, присвячений дослідженню цінностей, які найчастіше асоціюються з правом на захист персональних даних, у світлі нової тоталітарної загрози, яка підживлюється сучасними

цифровими тенденціями. *Богдан Карнаух* у своєму розділі досліджує право на забуття в ширшому контексті права на приватність, зосереджуючись на знакових справах та законодавчих змінах у Європі.

Тема 2 присвячена тому, як європейські фундаментальні цінності імплементовані в договірному та деліктному праві в цифрову епоху. Вона розпочинається зі статті *Наталії Філатової-Білоус*, яка аналізує сучасні тенденції договірного права та можливості горизонтального застосування європейських фундаментальних цінностей до договірних відносин у цифрову епоху. В розділі, підготовленому *Оксаною Кіріяк*, представлено глибокий аналіз багатогранного явища цифрового мовчання, розглядаються його визначення, прояви, правові наслідки, суспільна динаміка та етичні міркування. *Кирило Анісімов* у своєму розділі аналізує національне цивільне законодавство та практику щодо форми правочину, підпису та, певною мірою, порядку укладення договору, а також те, як воно враховує сучасні тенденції та виклики, спричинені цифровізацією.

Тема 3 присвячена імплементації європейських фундаментальних цінностей у процесуальне право в цифрову епоху. Вона починається з розділу *Наталії Сакари*, присвяченого дотриманню права на справедливий судовий розгляд при застосуванні інформаційних технологій у цивільному судочинстві. *Тетяна Цувіна* у своєму матеріалі розглядає потенційні можливості застосування ChatGPT у судочинстві, приділяючи особливу увагу його використанню учасниками судових процесів та їхніми адвокатами при підготовці процесуальних документів. *Оксана Капліна та Ірина Крицька* у своєму розділі визначають основні вектори цифрової трансформації кримінального процесу та аналізують їх з огляду на можливі переваги цифрових технологій у кримінальному судочинстві та потенційні ризики, які вони можуть нести.

Це книга у відкритому доступі, видана в рамках проєкту Центр Досконалості Жана Моне “Європейські фундаментальні цінності в цифрову еру”, EFVDE, (2022–2025), 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH, грантова угода 101085385, що співфінансується Європейським Союзом.

Сподіваємося, вам сподобається разом з нами досліджувати фундаментальні європейські цінності в цифрову еру. Ми раді будь-яким відгукам і запрошуємо кожного і кожну з вас до обговорення того, яке майбутнє чекає на людство.

Юлія Размєтаєва та Наталія Філатова-Білоус

European Fundamental Values in the Digital Age, a Prologue on the Societal Transformation of European Values

Stéphanie Laulhé Shaelou*

The book which the reader is about to enter and enjoy, is reflective of an interdisciplinary and multicultural research journey engaging with key socio-legal challenges in the digital world. Any meaningful journey must have a vision. A research journey is no exception. This book's vision appears to be *socio-legal-digital* one could say. As it emanates from a Jean Monnet Centre of Excellence on European Fundamental Values in Digital Era (EFVDE), working with our own Jean Monnet Centre of Excellence for the Rule of Law and European Values (CRoLEV), overarching desires are likely to be aligned, particularly seeing as Cyprus and Ukraine share common values and realities in Europe, including in troubled times. Via the consideration of European values in the digital world, Jean Monnet Centres of Excellence such as EFVDE or CRoLEV are key vehicles to participate to the digital enhancement of the rule of law, human rights and democracy in Europe and beyond, to contribute to overall societal harmony by deploying the digital aspects of society founded on European fundamental human rights and values with international reach. Through the study of the impact of digitization on European fundamental values and the enhancement of societal balances locally, with repercussions across Europe and beyond, such initiatives captured into this book wish to reflect on societal transformations and eventually contribute to sustainable justice beyond EU frontiers and concepts, into the digital world. Many

* Professor of European Law and Reform, Head School of Law and Director of the Jean Monnet Centre of Excellence for the Rule of Law and European Values CRoLEV, University of Central Lancashire Cyprus.

States in Europe but also worldwide have been heavily affected by emergency situations which have exacerbated global phenomena of social inequality, polarisation, misinformation, digital and societal transformations, all having a direct impact on modern societies and fundamental values. Ultimately, there is a need to advance European fundamental values into the digital world, of direct interest to any human being, generations to come, and societies, shifting focus from the conditionality to the sustainability of values.

As such, the concept of the 'European digital legal order' analysed elsewhere by the Directors of CRoLEV and EFVDE respectively[2] seems to enshrine the overarching concept of European legal order in a modern setting. The set of fundamental human rights, rule of law principles and democratic values traditionally enshrined in the post-modern multinational legal order are at the core of the digital transformation of principles, rights and values as considered in this book. From maintaining rule of law principles derive the sustainability of democratic values and freedoms under the law enshrined in fundamental human rights.[3] As argued at the premise of this book, "[t]o the extent that the European digital legal order is the manifestation of the European legal order in the modern digital world, the fundamental question of the nature, scope and upholding of fundamental human rights, Rule of Law principles and Democratic values remains".[4] This book is a daring attempt to enrich scholarship on European fundamental values in the digital ages and address their societal transformations in a socio-legal-digital context.

Pyla, Cyprus, August 2024

[2] S. Laulhé Shaelou and Y. Razmetaeva, 'Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values' (2023) 24(4) *ERA Forum* 567.

[3] Ibid, 567–8.

[4] Ibid, 568.

Theme 1
The concept of European fundamental values in the digital era: rights, principles and data

The Fundamental Values Triad in the Digital Age

Yulia Razmetaeva*

Abstract: Considering the confluence of technology, law, and societal dynamics, this chapter seeks to reveal both the opportunities and challenges regarding fundamental values in the digital age. A value triad of human rights, rule of law and democracy is a basis for European legal order and a 'beacon' for other legal systems. The digital age implications, including the consequences of certain technologies deployment, pose a serious threat to the values. In order to minimise threats and at the same time benefit from digitalization, we must act immediately. If no action is taken, the new technologies-centred philosophy might lead humankind to a rather dystopian future.

Keywords: fundamental values; human rights; rule of law; democracy; digital age; legal order; artificial intelligence; values erosion

1. A framework of fundamental values

A set of fundamental values form the basis of the European legal order and the European digital legal order[1], human rights, rule

* *Head of the Center for Law, Ethics and Digital Technologies and Associate Professor at the Department of Human Rights and Legal Methodology, Yaroslav Mudryi National Law University, Ukraine; Researcher at Centre for Multidisciplinary Research on Religion and Society, Department of Theology, Uppsala University, Uppsala, Sweden. Email: yu.s.razmetaeva@nlu.edu.ua*

[1] See S. L. Shaelou, Y. Razmetaeva, Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule

of law and democracy being the key values triad. An overarching document outlining these values does not yet exist and probably cannot exist. For the time being our understanding of the values is composed of the mosaics of concepts, principles and ideas contained in a whole range of legal acts, judicial decisions and legal doctrines.

Among thousands of documents mentioning the values in one way or another those that constitute the 'normative carcass' include the Universal Declaration of Human Rights[2] and the UN Charter[3] at the universal level, as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[4], the Council of Europe Statute[5], the Charter of Fundamental Rights of the European Union (EU Charter)[6], the EU Treaties[7] at the regional level. In turn, the key regional level is the European one, which represents a value-based and sufficiently effective regulatory framework that simultaneously has an authoritative impact that goes beyond direct jurisdictional force.

That being said, there does not appear to be a unified understanding of the term 'European', which might be regarded

of Law principles and European values, in ERA Forum, 24, 2023, 567–587, https://doi.org/10.1007/s12027-023-00777-2.

[2] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[3] Charter of the United Nations, 59 Stat. 1031, T. S. 993, 3 Bevans 1153, (26 June 1945), entered into force 24 October, 1945.

[4] European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 04 Nov. 1950), 312 E. T. S. 5, as amended by Protocol No. 3, E. T. S. 45; Protocol No. 5, E. T. S. 55; Protocol No. 8, E. T. S. 118; and Protocol No. 11, E. T. S. 155; entered into force 03 Sept. 1953 (Protocol No. 3 on 21 Sept. 1970, Protocol No. 5 on 20 Dec. 1971, Protocol No. 8 on 1 Jan 1990, Protocol 11 on 11 Jan 1998).

[5] Statute of the Council of Europe, E. T. S. 1, (5 May 1949), entered into force August 3, 1949.

[6] Charter of Fundamental Rights of the European Union, 2010 O. J. C 83/02, (18 December 2000), entered into force 01 December 2009.

[7] Consolidated Version of the Treaty on European Union [2008] OJ C115/13.

in geographical, political, cultural, etc. terms[8]. At the same time, it is rather clear that the key structures determining the term are the EU and the Council of Europe. The particular interpretations of concrete rights or principles may vary between the EU and the CoE; however, the fundamental triad is recognized in both.

Besides, there are two leading judicial institutions, namely the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) whose practice has a significant impact on the society's understanding of the values. A tendency can be observed of convergence of both courts' practice when interpreting the values and applying the corresponding principles. All listed above together constitute an almost imperceptible and indescribable but strong value base of the legal order and, in a broader sense, of European society.

In the digital age the foundations outlined above are shaken – the fundamental values are changing and being attacked.

2. The digital age as a time of unprecedented technological development

In an era defined by rapid technological advancement the values of human rights, democracy, and rule of law stand as guiding lights for peoples and societies navigating the complexities of the digital landscape. As digitalization permeates every aspect of life,

[8] See, e.g., G. Delanty, *Models of citizenship: Defining European identity and citizenship*, in *Citizenship Studies*, 1(3), 1997, 285–303, https://doi.org/10.1080/13621029708420660; T. Risse, *A European Identity? Europeanization and the Evolution of Nation-State Identities*, in M. Green Cowles, G. Caporaso and T. Risse (ed.), *Transforming Europe: Europeanization and Domestic Change*, Cornell University Press, Ithaca, 2001, 198–216; F. Wieacker, *Foundations of European Legal Culture*, in *The American Journal of Comparative Law*, 38(1), 1990, 1–29, https://doi.org/10.2307/840253; R. Münch, *Constructing a European Society by Jurisdiction*, in *European Law Journal*, 14(5), 2008, 519–541, https://doi.org/10.1111/j.1468-0386.2008.00428.x; P. Westerman, *Weaving the Threads of a European Legal Order*, in *Transboundary Legal Studies*, 8(3), 2023, 1301–1315, https://doi.org/10.15166/2499-8249/719.

it presents both unprecedented opportunities and significant challenges to these foundational values.

2.1. Why technological development affects everyone

Technologies in the digital age strive to become all-encompassing, permeating the whole picture of the world. In the past every new technology had to become embedded into the overall picture of the world. And it wasn't an easy process. In the nineteenth century, for example, electricity had to be inscribed into the religious picture of the world as a result of the efforts of people of many confessions. In contrast, these days technology is part and parcel of our lives. For many, life is unimaginable without technology. There is little rethinking, no pondering, no contemplation.

The array of new technologies and techniques – from the Internet, social media, artificial intelligence and mobile applications to keyword usage, web promotion and web design – is extremely wide and varied. No aspect of individuals lives remains untouched by them. The ubiquitous digitalization is altering our habits, daily routines, communication strategies, and what not. Moreover, people's online and offline lives have merged to the point of becoming inseparable.

The four manifestations of the digital age may influence individual's experience significantly today. The first digital age manifestation could be called 'digital neurotisation'. There are two phenomena that can contribute to it: the accelerated pace of life and the fight for people's attention. Today's technologies set a speedy pace of life: computers work increasingly quickly, data are processed and disseminated instantly, trends change like landscapes flickering behind the window of a high-speed train. In this turbulent maelstrom, it is increasingly difficult to grab people's attention, which is needed by companies, organisations and

governments. In trying to attract our attention they cram online and offline environments with more and more irritants (pop-up messages, loud noises, eye-catching advertisements, etc).

The trend of neurotisation is coupled with the trend of simplification. On the one hand, simplification could be the result of a conscious (intentional) influence that is carried out with the help of technology. Simplification, on the other hand, is part and parcel of the algorithms, which are occupying the private and public sphere of life embodied in artificial intelligence technologies. The complexity of algorithms has limits. An algorithm, moreover, will take into account only typical manifestations, a statistically relevant set of features, unable to handle the limitless complicacy of a personality. Every algorithm will inevitably simplify the image of a user. Any deviation from the standard model will be disregarded by it, seen as statistically irrelevant. For these two reasons, the multifaceted personality is replaced by a truncated, shallow one.

The third manifestation of the digital age that follows from the simplification, is categorisation, which leads to squeezing a complex set into a simplified framework. It is also part and parcel of the growth of algorithmic decisions and data processing. One example of that is tagging, which leads to categorization of complex stories. When applying a tag, we try to describe an event, however complicated, using a handful of keywords. Besides, by subscribing to a tag we fully subscribe to the entire phenomenon – even if our story is not one hundred percent relevant.

The fourth digital age manifestation could be called 'information fatigue'. We are bombarded with torrents of information on an hourly basis, which leads to mental exhaustion. Most people cannot be on the watch all the time. Therefore, on the one hand, even the most vigilant of us will buy into a fake every now and again. On the other hand, we can't resist the temptation to rely on our trusted sources without questioning, without a pinch of

salt. Yet, trusted sources can at times be mistaken. Another side of this 'informational fatigue' is what we can call 'numbness of mind', blurred vision. Since we simply can't absorb all the information we are exposed to, we just stop reacting to some of it, no matter how important it is. Issues really worthy of attention, such as outrageous rights violations, go unnoticed. It is becoming increasingly difficult for public interest organisations to raise people's awareness of problems that need urgent attention. In order not to be manipulated we need to be Jacks-of-all-trades, experts in every field. In order to assess the quality of the information we need to have time and mental capacity. But in the digital age, we have neither the former nor the latter.

Hannah Arendt reveales that technological progress turns the labouring society into a society of jobholders, that demands of its members nothing but automatic functioning, and all human activities "appear not as activities of any kind but as processes"[9]. With the four manifestations of the digital age suggested above, the trend towards automatic functioning can be greatly intensified.

Digital world and the dynamics of its growth influence every single individual despite the fact that the degree of its influence differs. Moreover, technological development has impacted – directly or indirectly – on the majority of individuals. People who are not using technologies might still be affected by them. Additionally, the changes in individual and collective experiences might be inconspicuous but irreversible. In particular, digital identity has born an unreasonably strong influence on human identity as such[10]. Online activities

[9] H. Arendt, *The human condition*, The University of Chicago Press, Chicago & London, 1998, 322.

[10] See P. Nagy, B. Koles, *The digital transformation of human identity: Towards a conceptual model of virtual identity in virtual worlds*, in *Convergence*, 20(3), 2014, 276–292, https://doi.org/10.1177/1354856514531532; S. Çöteli, *The Impact of New Media on The Forms of Culture: Digital Identity and Digital Culture*, in *Online Journal of Communication and Media Technologies*, 9(2), 2019, e201911; A. Beduschi, *Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations*, in *Data & Policy*, 31, 2021, e15, https://doi.org/10.1017/dap.2021.15.

and social media gradually and imperceptibly change our ideas of ourselves. The images that one shares in cyberspace are cemented by an incredibly long digital footprint. The images others share can be far from the truth or intentionally fragmented. Other examples are connectivity as well as digital representation. Disconnecting is becoming increasingly impossible: both from the point of view of individual habits and social expectations. Deleting parts of digital personality means literally vanishing from the memory of others and even online mediated social life. There are many more examples of how the digital age and its technologies are changing the human experience, but it is quite clear that these changes are consequential and far-reaching.

The digital age built on technologies has features that significantly change the experience of individuals and communities. The four manifestations of the digital age – 'digital neurotisation', simplification, categorisation, and 'information fatigue', exacerbated by the growing algorithmisation, – may aggravate polarisation of opinions and deepen societal divides, undermine democracy and justice, erode fundamental rights. What's more, certain technologies' almost imperceptible impact can change the very way individuals think and perceive reality.

2.2. Why technologies are not merely neutral tools

Although today's technologies construct our experience in a way entirely different from the past, people are still unprepared to estimate their hidden dangers. Humans are still used to thinking of any technology as merely a tool, and when the tool promotes the violation of fundamental rights as well as an intervention in democracy and justice, we are still inclined to think that it's the evil hands, not the tool, which are to blame. However, as it seems, today's technologies are much more than merely tools. There are at least three reasons why technologies should not be regarded as such merely tools, neutral and de-personalised: (1) the 'creator

bias', (2) the non-neutral nature of certain technologies, especially artificial intelligence, and (3) the dramatically increased possibilities for technologies to influence people, especially their opinions.

The first reason has to do with how technologies reflect the preconceptions of their creators. Smart algorithms are a good example. Seemingly impartial and accurate, they, in fact, very often happen to replicate and augment biases. When compiled by a biassed creator, the algorithms won't be but biassed as well. The data we feed AI may not sufficiently represent vulnerable groups or may bear the imprint of past discriminatory practices. This is well illustrated by the biases in AI designed for litigation, like, racist algorithmic decisions based on court cases collected over the years, where the statistics of decisions made by white people were not in favour of blacks[11]. If there is insufficient control and monitoring of the bias of the creators, the result of creation can be a significant threat for people and societies.

The second reason revolves around the question of whether technologies are neutral by nature. Presumably, some elements of digital technologies are inherently manipulative. The manipulative design of landing pages is aimed at getting people to press the "purchase" button. Overly user-friendly websites, seamless and smoothly taking individuals from bullet point to bullet point, reduce our urge to check and doubt. A friendly interface and apparent convenience all contribute to the fact that we delve less into what is happening, rely more on someone else's choices and trust other people's opinions more. Ultimately, this can narrow the scope of our autonomy. Search engines, returning different results for the same query for different users depending on what they previously defined as their preferences, are often intentionally or unintentionally biassed. Yet, people still tend to think of a search engine as just that – an engine, a tool, failing to see the manipulator behind it.

[11] J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias*, 23 May 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Michael Klenk wrote: "First, digital behavioural technologies can be studied as tools wielded by humans or firms, and questions about manipulation would concern whether these tools are used in a manipulative way. Second, digital behaviour technologies – which sometimes operate autonomously (such as a recommender system designed to keep users engaged) – may themselves be considered as agents of manipulation"[12]. According to Lucas Miotto and Jiahong Chen, the technology of "real-time profiling" is manipulative and dangerous, and designed to have the capacity of predicting certain transient and dynamic characteristics of a user at an exact moment[13]. This type of profiling involves psychological hijacking and works as a gateway to further wrongs by catching users in their vulnerable states. The EU Artificial Intelligence Act, for example, prohibits the real-time profiling[14], however, jurisdictional restrictions and balanced limitations of AI development are unlikely to prevent this completely and everywhere.

The newsfeed curator algorithms in social media filter off part of content based on ambiguous and obscure rules[15]. Users are intentionally exposed to a large amount of negative news and radical opinions in order to evoke stronger reactions and harvest more "hate clicks"[16]. Most of the algorithms, tuned to keep us online and engaged, are set to detect affective reactions. If hate

[12] M. Klenk, *(Online) manipulation: sometimes hidden, always careless*, in *Review of Social Economy*, 80(1), 2022, 86, https://doi.org/10.1080/00346764.2021.1894350.

[13] L. Miotto, J. Chen, *Manipulation, Real-time Profiling, and their Wrongs*, in M. Klenk and F. Jongepier (ed.), *The Philosophy of Online Manipulation*, Routledge, New York, 2022, 392–409, https://doi.org/10.4324/9781003205425-24.

[14] 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.

[15] *The invisible curation of content: Facebook's News Feed and our information diets, The Web Foundation*, Report authored by R. Ávila, J. Ortiz Freuler and C. Fagan. Washington, 2018. http://webfoundation.org/docs/2018/04/WF_InvisibleCurationContent_Screen_AW.pdf.

[16] K. Way, *Hate Clicks Are the New Clickbait*, 20 February 2019. https://contently.com/2019/02/20/hate-clicks/.

speech elicits a stronger reaction, it will, in all likelihood, be used in one way or another, despite all the assurances of the social media managers about their efforts to root violence out. Paradoxically, the counter-trend is even worse. If people try to fight with hate speech by algorithmic censorship, AI technologies erase pieces of harmless content because they understand it too literally.

Daniel Susser, Beate Roessler and Helen Nissenbaum argue that certain technologies, for a number of reasons, make "engaging in manipulative practices significantly easier, and it makes the effects of such practices potentially more deeply debilitating"[17]. The SMM technology, for instance, is aimed at twisting the sales funnel and it doesn't care what it sells and imposes – certain types of tea and coffee or certain religious and political views.

The third reason to consider today's technologies non-neutral and not-just-tools is the dramatically increased possibilities for them to influence people. For example, technologies fundamentally increase the ability of their owners and developers to manipulate human "likings"[18] when advertising something. The combination of high-level profiling, tracking of a person's actions, and algorithmic recommendations aimed specifically at that person makes such advertising extremely successful in getting that person to buy what is being promoted. This can apply not only to some 'small' choice, such as buying garden furniture at a specific manufacturer, but also to the 'big' choice of political affiliation and, accordingly, the individual who will lead the state for the next few years.

Apart from that, many new technologies are unpredictable and, therefore, dangerous. Joyfully playing with ChatGPT, we can miss the fact that the habit of trusting the rewriting of texts by AI

[17] D. Susser, B. Roessler, H. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, in *Georgetown Law Technology Review*, 4 , 2019, 1–45, 3.

[18] See A. Barnhill, *I'd Like to Teach the World to Think: Commercial Advertising and Manipulation*, in *Journal of Marketing Behavior*, 1 (3–4), 2016, 307–328, http://dx.doi.org/10.1561/107.00000020.

and not our own mind can take us far. Probably so far that we will lose the ability to reflect and to have an inner monologue. It would be naive to think that such fundamental changes in the lives of people and societies caused by breakthrough technologies will not be reflected in the triad of fundamental values.

3. Human rights, democracy and the rule of law in the digital era

3.1. Human rights in the digital age: conceptual changes and key challenges

Human rights, enshrined in international and national legal acts, serve as the cornerstone of a just and equitable society. In the digital age, these rights extend beyond the physical realm into the virtual space, empowering and endangering human beings at the same time.

One of the most serious changes regarding this fundamental value in the digital age is the emergence of digital human rights. There are different terms playing around this topic, including "digital rights"[19], "digital rights and freedoms"[20], "digital liberties"[21], etc. A number of authors have been exploring "human rights in the digital

[19] See K. Karppinen, O. Puukko, *Four discourses of digital rights: Promises and problems of rights-based politics*, in *Journal of Information Policy*, 10, 2020, 304–328, https://doi.org/10.5325/jinfopoli.10.2020.0304; G. Goggin, et al., *Data and digital rights: recent Australian developments*, in *Internet Policy Review*, 8(1), 2019, https://doi.org/10.14763/2019.1.1390; L. Pangrazio, J. Sefton-Green, *Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?*, in *Journal of New Approaches in Educational Research*, 10, 2021, 15–27, https://doi.org/10.7821/naer.2021.1.616.

[20] See L. Taylor, *What is data justice? The case for connecting digital rights and freedoms globally*, in *Big Data & Society*, 4(2), 2017, https://doi.org/10.1177/2053951717736335; A. Pettrachin, *Towards a universal declaration on internet rights and freedoms?*, in *International Communication Gazette*, 80(4), 2018, 337–353, https://doi.org/10.1177/1748048518757139; B. Custers, *New digital rights: Imagining additional fundamental rights for the digital era*, in *Computer Law & Security Review*, 44, 2022, 105636, https://doi.org/10.1016/j.clsr.2021.105636.

[21] G. Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, Springer, Dordrecht, 2013, 39.

age"[22], delving into the existing fundamental rights and coming up with novel ideas as to how they transform under the influence of technological development, while at the same time looking into the digital aspect of their implementation and protection.

Since 'digital rights' has been used to refer to different variations of rights, values and guiding lights, it is difficult to define what they are. At the same time, they could be considered in three dimensions: (1) as special rights arising from fundamental and formed in the digital age; (2) as those fundamental rights that are especially important today in connection with the development of information and communication technologies; (3) as human rights when they areexercised in the digital environment[23].

Therefore, conceptual changes can relate to both the understanding of the essence of human rights and the expansion of their catalogue. Along with that, the ways the rights are implemented also transform; new ways of rights protection are worked out. This in turn may be embodied in the emergence of new (or renewed) individual rights. The latter entails discussions about whether such rights as the right to be forgotten, the right not to be subjected to automatic processing, the right to the Internet, the right to data protection, etc., can be regarded as 'human rights' today, that is, as those that have reached the status of fundamental.

[22] See, e. g., K. Mathiesen, *Human Rights for the Digital Age*, in *Journal of Mass Media Ethics*, 29(1), 2014, 2–18, https://doi.org/10.1080/08900523.2014.863124; J. Coccoli, *The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era*, in *Peace Human Rights Governance*, 1(2), 2017, 223–250, https://doi.org/10.14658/PUPJ-PHRG-2017-2-4; Yu. Razmetaeva, Yu. Barabash, D. Lukianov, *The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice*, in *Access to Justice in Eastern Europe*, 3(15), 2022, 41–56, https://doi.org/10.33327/AJEE-18-5.3-a000327.

[23] Yu. Razmetaeva, Yu. Barabash, D. Lukianov, *The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice*, cit., 47.

In particular, the right to data protection is already enshrined as one of the fundamental rights in the EU Charter[24]. Stemming from the Charter, the recent European Declaration on Digital Rights and Principles for the Digital Decade[25] recalls the freedom of expression and information, data protection and privacy, while at the same time proposing to consider as vital the right to access (digital connectivity), the right to digital education and the right to safe and secure digital environment.

Another trend regarding human rights in the digital era is the asymmetry of power and impact. It is practically impossible not to recognise that certain actors' impact on human rights has increased significantly. This fuels the debate about the need to expand the range of human rights addressees and place more responsibility on powerful players[26]. The discussion about the need to impose additional obligations on these players initially focused mainly on transnational corporations and, sometimes, international organisations. In the digital era, it shifted towards the understanding that additional responsibility should be placed on big tech companies, especially the owners of large digital platforms. Taking into account the fact that some technological tools can give great power even to small companies, it seems

[24] Charter of Fundamental Rights of the European Union, cit.

[25] European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01).

[26] See, e. g., J. G. Ruggie, *Just Business. Multinational Corporations and Human Rights*, Amnesty International Global Ethics Series, W. W. Norton & Company, New York, 2013; A. Ramasastry, *Corporate Social Responsibility Versus Business and Human Rights: Bridging the Gap Between Responsibility and Accountability,* in *Journal of Human Rights*, 14 (2), 2015, 237–259; B. Santoso, *Just Business – Is the Current Regulatory Framework an Adequate Solution to Human Rights Abuses by Transnational Corporations?* In *German Law Journal*, 18(3), 2017, 533–558, https://doi.org/10.1017/S2071832200022057; S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019; B. J. Sander, *Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law*, in *European journal of international law*, 32(1), 2021, 159–193.

that the circle of those responsible should include all business entities.

There are a number of decisions of the European Court of Human Rights that deal with various violations of fundamental rights related to digital technologies, as well as the activities of companies. These decisions often contain important positions about the scope of these rights and the legitimate expectations of individuals. For example, there is a well-known case where a company fired an employee based on tracking their email messages and accessing their content; however, the employee was not informed of the nature or extent of the surveillance or the degree of intrusion into his privacy and correspondence[27]. A number of positions have emerged on how accessing YouTube as a single platform which enabled information of specific interest, particularly on political and social matters helps to ensure freedom of expression[28], how important the hyperlinks for the smooth operation of the Internet[29], that is, for expressing the opinions and exchanging information there, and how the provision by a political party a web application for voting is an exercise of the freedom of expression[30]. Some decisions concern those actors, including companies, which allegedly only provide platforms for commenting on the Internet and try to avoid the responsibility inherent in "publishers"[31]. This is only a small range of the cases

[27] European Court of Human Rights (Grand Chamber) Judgment. Bărbulescu v. Romania. App. Nos. 61496/08 (2017).

[28] European Court of Human Rights Judgment. Cengiz and Others v. Turkey. App. Nos. 48226/10, 14027/11 (2015).

[29] European Court of Human Rights Judgment. Magyar Jeti Zrt v. Hungary. App. Nos. 11257/16 (2018).

[30] European Court of Human Rights (Grand Chamber) Judgment. Magyar Kétfarkú Kutya Párt v. Hungary. App. Nos. 201/17 (2020).

[31] See European Court of Human Rights (Grand Chamber) Judgment. Delfi AS v. Estonia. App. Nos. 64569/09 (2015); European Court of Human Rights Judgment. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary. App. Nos. 22947/13 (2016).

that are related to the use of new technologies, but they all show how difficult it is to keep fundamental rights intact and how ambiguous it becomes to understand their essence by different actors of legal order in the digital era.

While it cannot be said that people are missing out on the existence of the threats to human rights in the digital age altogether, the scale of these threats seems to be underestimated. Above all, fundamental rights are under attack; those that are the key to securing many other human rights: privacy and freedom of expression. Serious and in addition poorly tracked threats undermine the right to non-discrimination, which is the basis for the protection of other individual rights.

New threats to human rights are emerging from the rise in profiling and automation of data processing, as well as the introduction and deployment of assistive algorithms and AI-based decision-making. In particular, by increasing the share of artificial intelligence in service delivery, companies are not always doing due diligence or diversity. Thus, discriminatory practices become increasingly difficult to track down.

For example, the landmark lawsuit "State v. Loomis"[32] on the application of an algorithm to assess risk in sentencing shows that developers are not inclined to reveal all the secrets of what lies at the heart of decisions based on artificial intelligence. In addition, due to deliberate or unconscious underestimation of the possible consequences, business structures often do not see which genie is released (or may be released) from the bottle.

It is important to mention that many of the new threats to human rights are hidden and the negative consequences can have an effect far delayed in time. This makes the risks to human rights of introducing certain digital technologies difficult to predict. All

[32] State v. Loomis, 881 N. W.2d 749 (2016).

these threats are also constantly evolving in an unpredictable way, because the development of digital tools has no common plan. In a sense, they open the door to other dangers and other problems, the consequences of which can be irreparable.

Addressing these challenges requires robust legal frameworks, international cooperation and technological innovation to safeguard human rights in the digital realm. Correspondingly, it requires a broad understanding by the rights holders of what is happening to human rights, as well as a broad cooperation of various professional fields representatives to implement a long-term and effective strategy for combating threats.

3.2. Democracy in the digital era: openness, manipulation, and polarisation

Democracy thrives on principles of citizen participation, transparency, and accountability. The digital age has democratised access to information and facilitated new forms of civic engagement, empowering individuals to organise, advocate, and hold their governments accountable like never before. However, the same digital technologies that empower citizens also present challenges to democratic governance. The spread of online misinformation, manipulation of social media algorithms, algorithmic censorship marking the rise of digital authoritarianism throughout[33] threaten to undermine democratic institutions and processes.

Today's technologies can significantly enhance individuals' or groups' impact, enabling successful preaching to millions and making the opinions of a few vitally important to many. Such popularity, however, will not be the result of any outstanding wisdom or spiritual value, but merely the outcome of efficiently applying technical tools – the tools that have imperceptibly but

[33] See G. Gosztonyi, *The Rise of Digital Authoritarianism Across the Globe*, in *Censorship from Plato to Social Media. Law, Governance and Technology Series*, 61, 2023, 157–168.

firmly entered our lives while we underestimate the hazards of some of them, overwhelmed by their obvious advantages.

Technologies result in forming what could be called 'package perception': a kind of perception which doesn't distinguish shades and doesn't understand atypical combinations of characteristics. It manifests itself in trying to adjust an unconventional reality to the conventional norms. As an example, there exists a conventional image of a typical democrat and a typical republican. A democrat will drive a hybrid, drink latte, eat healthily, and be tolerant to religions. A republican will drive a Land Rover, drink beer, eat junk food, and be a firm protestant. As Asma Uddin believes, now we can see the partisan divide on religion and we also see growing partisanship on the issue of religious freedom.[34] She explains it by the paradigm of American "Mega-identity", concept of which was offered by Lilliana Mason,[35] when partisan affiliations morphed into identities. What's more, the identities include a whole host of things that have nothing to do with social policy. For instance, Muslims and Christians are described as belonging to opposing political camps. In addition, Christians (mostly white and conservative) are associated with the Republican Party, while religious minorities, particularly Muslims, are associated with the Democratic Party. What brought this mega-identity phenomenon about? It seems that technologies played a significant role in the aggravation of this divide by creating opinion bubbles and promoting "package images".

This is proved by, for instance, the Cambridge Analytica case in which the data of 50 – the figure which later went up to 87,[36] –

[34] A. Uddin, Why political polarization is a threat to Americans' religious liberty, 13 April 2021. https://www.usatoday.com/story/opinion/2021/04/13/how-political-polarization-threatens-religious-liberty-america-column/7186482002/

[35] L. Mason, *Uncivil Agreement: How Politics Became Our Identity,* University of Chicago Press, Chicago, 2018.

[36] I. Manokha, *Surveillance: The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective*, in *Theory & Event*, 21 (4), 2018, 891–913.

million users made it possible to determine with a lot of precision their political preferences before the elections, and even estimate the numbers of those who doubted which side to take. This campaign, as Pelin Vardarlier and Cem Zafer write, has played a serious role in the US elections and shifted the political balance[37]. Later on, users belonging to each camp were exposed to the selected information typical of this camp. This strengthened their desire to lean to one side, while encouraging intolerance of the representatives of the other.

According to Jim Isaak and Mina J. Hanna, governance institutions demonstrably lack the capacity to anticipate technology's future impact on the individuals' rights, structure of society, ideological divides, and political schisms among its citizens and the expansion of identity politics[38]. Big data and sophisticated analytic algorithms make it relatively easy for stakeholders to define our preferences, successfully profiling and targeting us. Since the goal is to keep us engaged and sell us something (goods, services, or views), personality traits are classified and processed to create a series of typical images, which are subsequently simplified for algorithms to process them, before being instilled in us. The artificially created images start replacing our own perceptions, becoming a new reality. As a result, intolerance grows towards those who deviate from these images. Artificially altered perceptions and imposed preferences, together with political profiling, create one of the most significant threats to democracy today.

Another significant threat to democracy in the digital age is a replacement of deeply-rooted and firmly established governance by algorithmic governance. This shift manifests itself in the variety

[37] P. Vardarlier, C. Zafer, *Social Media and Crisis Management: The Case Study of Cambridge Analytica*, in *Celal Bayar University Journal of Social Sciences*, 18 (Özel Sayı), 2020, 31–44.

[38] J. Isaak, M. J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, in *Computer*, 51 (8), 2018, 56–59.

of ways: AI-based decision-making in public administration[39], automated requests processing, algorithmic content moderation[40] and chat bots[41] used by official government sites, etc. Algorithmic governance risks undermining the foundations of governance and trust in public institutions as such. The thought and behaviour control by means of new technological tools has extremely negative consequences for democracy. Depersonalisation is one of the deplorable effects of the above-mentioned tendencies.

Another worrying trend is the acquisition of public power by private entities. This stems from and couples with the transformation of public and private spheres[42] in the digital age.

[39] See M. Kuziemski, G. Misuraca, *AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings*, in *Telecommunications Policy*, 44 (6), 2020, 101976, https://doi.org/10.1016/j.telpol.2020.101976; B. W. Wirtz, J. C. Weyerer, C. Geyer, *Artificial Intelligence and the Public Sector – Applications and Challenges*, in *International Journal of Public Administration*, 42 (7), 2019, 596–615, https://doi.org/10.1080/01900692.2018.1498103; M. Nordström, *AI under great uncertainty: implications and decision strategies for public policy*, in *AI & Society*, 37, 2022, 1703–1714, https://doi.org/10.1007/s00146-021-01263-4.

[40] See R. Gorwa, R. Binns, C. Katzenbach, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in *Big Data & Society*, 7 (1), 2020, 1–15, https://doi.org/10.1177/2053951719897945; Yu. Razmetaeva, *Algorithms in the activity of digital platforms*, in *Ekonomichna teoriia ta pravo – Economic Theory and Law*, 3(54), 2023, 93–104, https://doi.org/10.31359/2411-5584-2023-54-3-93; N. Filatova-Bilous, *Content moderation in times of war: testing state and self-regulation, contract and human rights law in search of optimal solutions*, in *International Journal of Law and Information Technology*, 31(1), 2023, 46–74, https://doi.org/10.1093/ijlit/eaad015.

[41] See N. Maréchal, *When Bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites*, in *International Journal of Communication*, 10, 2016, 5022–5031; Z. Engin, P. Treleaven, *Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies*, in *The Computer Journa*, 62(3), 2019, 448–460, https://doi.org/10.1093/comjnl/bxy082; N. Aoki, *An experimental study of public trust in AI chatbots in the public sector*, in *Government Information Quarterly*, 37(4), 2020, 101490, https://doi.org/10.1016/j.giq.2020.101490; M. de S. Monteiro, G. O. da S. Batista, L. C. de C. Salgado, *Investigating usability pitfalls in Brazilian and Foreign governmental chatbots*, in *Journal on Interactive Systems*, 14(1), 2023, 331–340, https://doi.org/110.5753/jis.2023.3104.

[42] See A. Jungherr, R. Schroeder, *Digital Transformations of the Public Arena*, Cambridge University Press, Cambridge, 2022; Y. Razmetaeva, *Digital platforms and their*

Digital platforms and those behind them formally belong to the private sector of society. However, this is not how things are in reality. The domination and omnipresence of private actors in digital environments[43] has endowed them with next to unlimited power in the epoch when digital environments have become the integral parts of social life: take social media, search engines, marketplaces as examples. While having become, in fact, part of the government, they are still reaping all the benefits allowed to private entities, which is a self-contradictory arrangement.

Besides, those private actors who owned digital platforms and developed new technologies, make efforts to recklessly accelerate technological development, which differs from a reasonable, and not only purely economically justified approach. In addition, in most cases, these entities, as well as their owners and managers, avoid responsibility for how their activity affects human rights, democracy and the rule of law. As Koen Frenken and Lea Fuenfschilling write, "platforms manage their workforce with a capacity similar to traditional corporations and in the interest of its investors, but without the formal obligations that traditional corporations face regarding their employees and other stakeholders"[44]. The problem of the responsibility of digital platforms deepens both against the background of their growing power as owners of new technologies

normative role: looking through the lens of European fundamental values, in *Pravo i suspilstvo*, 4, 2023, 38–44. https://doi.org/10.32842/2078-3736/2023.4.7.

[43] See, e.g., B. Love, *The Increasing Power of Tech Giants*, in C. Bissinger (ed.), *Tech Giants and Digital Domination*, Greenhaven Publishing, New York, 2018, 17–21; B. Valtysson, *Facebook as a Digital Public Sphere: Processes of Colonization and Emancipation*, in *tripleC*, 10(1), 2012, 77–91, https://doi.org/10.31269/triplec.v10i1.312; K. Birch, D. Cochrane, *Big Tech: Four Emerging Forms of Digital Rentiership*, in *Science as Culture*, 31(1), 2021, 44–58, https://doi.org/10.1080/09505431.2021.1932794; R. Fischli, *Citizens' Freedom Invaded: Domination in the Data Economy*, in *History of Political Thought*, 43(5), 2022, 125–149.

[44] K. Frenken, L. Fuenfschilling, *The Rise of Online Platforms and the Triumph of the Corporation*, in *Sociologica*, 14(3), 2020, 103, https://doi.org/10.6092/issn.1971-8853/11715.

and against the background of the fact that they often operate in areas where traditional legal safeguards and measures are not sufficiently effective.

The algorithms of digital platforms are geared towards retaining attention and greater involvement, often overlooking ethical business conduct in pursuit of these goals. They use not only an aggressive business model, but also shaping digital space and the visibility of something or someone in the agenda. Whatever is not in today's agenda is almost non-existent in the minds of people. In addition, the way in which algorithms attract and retain attention and how they shape the agenda is opaque, hidden from the public.

As it was rightly noted, "there is an assertive force about digital platforms able to transform the world in ways specific to their logics of operation"[45]. This power could have been directed to the promotion of values and their support. For some time it seemed that it was so. For example, social media platforms seemed to be good spaces and tools for democratic discussions, unity of like-minded people, organisation of protests in situations that required immediate public response. However, this turned into a powerful manipulation of users' opinions that spread far beyond the borders of digital spaces, polarisation and radicalisation, as well as the growing dependence of public opinion and public institutions on seemingly private digital platforms.

It is worth mentioning that decision-making based on smart algorithms is gaining momentum at all levels and is penetrating the private and public spheres. In this sense, platforms make a significant contribution to forming the habit of such decisions. This applies both to individual decisions that are made on the basis of algorithmic recommendations by people regarding their

[45] N. Rossiter, S. Zehle, *Platform Politics and a World Beyond Catastrophe*, in Armano, E., Briziarelli, M., and Risi, E. (eds.), *Digital Platforms and Algorithmic Subjectivities*, London: University of Westminster Press, 2022, 34, https://doi.org/10.16997/book54.c.

life choices, and to decisions that are made at the level of a community or an entire society and that partially or completely rely on algorithmic calculations.

Digital platforms are pushing societies towards total algorithmisation. One of the mechanisms of such pushing is the production and promotion of such content and, in a broader sense, such forms of expression that are easily recognized and processed by algorithms. According to Tarleton Gillespie: "There is a powerful and understandable impulse for producers of information to make their content, and themselves, recognizable to an algorithm. A whole industry, search engine optimization (SEO), promises to boost websites to the top of search results"[46]. For example, the texts we read online today are often designed in such a way that they are better not for humans but for algorithms. This can be achieved with the help of certain text structuring, the use of keywords that help bring the content higher in the search results, translations performed automatically and on the basis of AI tools.

It should be noted that one of the serious dangers of algorithmic governing, which has negative consequences for democracy and human rights, is the gradual elimination of people from processes, including decision-making processes. In the context of algorithmic disclosure co-regulation for platforms' business users, Fabiana Di Porto and Marialuisa Zuppetta argued that: "The human presence […] is essential to monitor if errors occur in the building of the knowledge graph: technicians supervising in the sandbox may intervene to eventually deactivate any error that may occur in the algorithm"[47]. There is no way we can adjust the algorithm once and for all, leaving it in the future without human intervention, and

[46] T. Gillespie, *The Relevance of Algorithms*, in T. Gillespie, P. J. Boczkowski, and K. A. Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MIT Press, 2013, 184.

[47] F. Di Porto, M. Zuppetta, *Co-regulating algorithmic disclosure for digital platforms*, in *Policy and Society*, 40(2), 2021, 287, https://doi.org/10.1080/14494035.2020.1809052.

get the results of this algorithm's activity that would correspond to fundamental values requirements. Firstly, the challenges that arise at the level of communities and societies are always dynamic, so certain elements of values can be revised or applied differently in different contexts. Secondly, it is necessary to monitor the algorithms to see if there are any biases or errors, since this cannot always be detected before the deployment of a particular algorithm. This also applies to human supervision of embedded technologies in terms of revising social practices. For example, these can be practices that algorithms follow or learn from, but which we currently consider or will consider unacceptable at some point (discriminatory, illegal, etc.). Thirdly, the variability of life circumstances is higher than any today's algorithm can take into account while working effectively. This means that there will be cases that will not be handled correctly by the algorithms because they deviate and that human supervision should at least follow up on such rare cases and solve them manually.

Undoubtedly, there must be a fair balance between innovation and the protection of values. At the same time, algorithmic governing and the application of technologies as such are not always what should be implemented as soon as possible, even if the real or declared goal is to promote, ensure and protect fundamental values and their elements. In particular, to eliminate discrimination in the workplace, hiring algorithms are used instead of in-person interviews. Parsing algorithms then withdraw all who are not giving their CV in proper machine-readable form. However, instead of contributing to the reduction of discrimination, such technological solutions may lead to its growth. They also can contribute to the emergence of new forms of inequality like an algorithmic discrimination, as it was in the well-known case with the Amazon hiring algorithm that learned from past discriminatory practices and created a pattern to hire men for some positions

and not to hire women for these positions. With the growth of algorithmic governing, there will be more and more such cases.

The issue of content censorship in the digital age is not new, however, it acquires new connotations against the background of digital platforms (and their owners) wide implementation of algorithms, especially content moderation algorithms. Jennifer Cobbe argues that: "the emergence of extensive algorithmic censorship as a primary form of content moderation by social media platforms is an unwelcome development that gives rise to new forms of corporate societal authority"[48]. She writes that it not only increases the power of the platforms but also enables them to insert commercial considerations into everyday communication between people.

Platforms regulate the understanding of what is freedom of speech and hate speech, relying primarily on their own rules, neither on human rights conventions, pacts or other legal acts, nor on legal doctrines established in the practice of authoritative international and national judicial institutions. In addition, they do not have mechanisms for balancing rights in conflict situations, which can be found in national and international law, and adjusted in line with judicial practice. Certainly, platforms can set rules, but they also have the properties of a public forum, especially in an environment where it is extremely important to convey an opinion and when this remains the only channel of communication. That raises the question of proportionality, balancing freedom of expression with other human rights, and in a broader sense the question of fundamental values.

The rapid dissemination of false or misleading information through social media platforms, online news outlets, and other digital channels has the potential to distort public discourse, manipulate electoral processes, and undermine trust in democratic

[48] J. Cobbe, *Algorithmic Censorship by Social Platforms: Power and Resistance*, in *Philosophy & Technology*, 34, 2021, 743, https://doi.org/10.1007/s13347-020-00429-0.

institutions. Moreover, the viral spread of misinformation exacerbates social polarisation and erodes the shared understanding necessary for democratic deliberation and decision-making.

Technologies facilitate the practice of deliberative democracy by providing platforms for informed and reasoned public deliberation on complex policy issues. Through online forums, virtual deliberative assemblies, and collaborative decision-making platforms, citizens can engage in substantive dialogue, exchange diverse viewpoints, and co-create solutions to pressing societal challenges. In parallel, technologies allow certain actors to add fuel to the fire: normalising undemocratic processes and deepening social division. For instance, the algorithmic curation of online content poses significant risks to democracy by reinforcing filter bubbles and echo chambers that insulate individuals from diverse perspectives and alternative viewpoints. As social media platforms and search engines prioritise content based on user preferences and engagement metrics, they inadvertently amplify partisan narratives, polarise public discourse, and foster a fragmented media system devoid of shared facts or common ground.

Preserving democracy in the digital era requires a multifaceted approach that combines regulatory measures, media literacy initiatives, and civic education efforts. This should be a joined effort, but there should also be an honest recognition of the fact that democracy deteriorates under algorithmic governance. There should also be a fair judgement of the asymmetry of power, especially the power that apparently private actors have in the public sphere.

3.3. The rule of law in the digital age: preserving the sense of justice

The rule of law serves as the bedrock of democratic societies, ensuring that all individuals, regardless of their status or power,

are subject to transparent legal processes and equal treatment. As Kim Lane Scheppele rightly points out, the rule of law has also become key for "holding political power accountable"[49].

Despite the fact that the definition and elemental composition of this value are the subjects of serious debate, the definition proposed by the Venice Commission[50] might be a starting point for consensus. In the case of its adoption, it would be necessary to consider such rule of law elements as (1) legality, (2) legal certainty, (3) prevention of abuse/misuse of powers, (4) access to justice, and (5) equality before the law and non-discrimination. The listed elements, in turn, consist of smaller elements, or indicators. For example, such an element as 'access to justice' includes independence and impartiality, which, among other things, comprise independence of the judiciary, independence of individual judges, and impartiality of the judiciary.

The rule of law is undoubtedly vital for societies that are or aspire to be democratic, able to effectively protect individual rights, preventing or minimising state arbitrariness and the abuse of power in a broad sense. This value and at the same time the legal principle, if firmly rooted and maintained at the proper level, contribute to the stability of society and resilience in the face of dangers. However, in the digital age, the rule of law faces unprecedented challenges[51] caused by emerging technologies,

[49] K. L. Scheppele, *The Life of the Rule of Law*, in *Annual Review of Law and Social Science*, 20, 2024, https://doi.org/10.1146/annurev-lawsocsci-010924-103836.

[50] Report on the rule of law. Adopted by the Venice Commission at its 86th plenary session (Venice, 25–26 March 2011). CDL-AD(2011)003rev-e. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e.

[51] See, e.g., T. Kerikmäe, K. Nyman-Metcalf, *The Rule of Law and the Protection of Fundamental Human Rights in an Era of Automation*, in J.-S. Gordon (ed.), *Smart Technologies and Fundamental Rights*, Brill, Leiden, 2020, 221–239, https://doi.org/10.1163/9789004437876_011; N. Susor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, in *Social Media + Society*, 2018, https://doi.org/10.1177/2056305118787812; S. L. Shaelou, Y. Razmetaeva, *Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems:*

especially artificial intelligence,[52] and the consequences of their use, which may contribute to destroying this value completely.

The number of influences on independence and impartiality, in particular, is enormous and increasing day by day, which can be observed on a 'personal' and 'public' levels[53]. On a personal level, judges and juries, like other people, are involved in the digital space to some extent today. They may have social media accounts and leave digital footprints that make it easier, for instance, to deeply profile them obtaining detailed pictures of their personal lives. This, in turn, is used to strategise in litigation based on the vulnerabilities of specific decision makers. At the public level, digital tools, especially algorithms, make it relatively easy, – far easier than in pre-digital epochs, to manipulate public opinion. They allow, for example, certain opinions about judicial processes to be widely disseminated, imbued with certain doubts and certain emphases, to influence both the decision-makers and the public expectations of those decisions. This is especially important with high-profile cases with broad publicity or significant political implications.

Thus, we need to recognise that the judge who makes the decision and gives the verdict is exposed to far more influences and attempts at influence through technology today than two decades

shaping the digital legal order while upholding Rule of Law principles and European values, cit., 567–587.

[52] See M. Hildebrandt, *Algorithmic regulation and the rule of law*, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376 (20170355), 2018, http://dx.doi.org/10.1098/rsta.2017.0355; S. Rosengrün, *Why AI is a Threat to the Rule of Law*, in *Digital Society*, 1(10), 2022, https://doi.org/10.1007/s44206-022-00011-5; S. Greenstein, *Preserving the rule of law in the era of artificial intelligence (AI)*, in *Artificial Intelligence and Law*, 30, 2022, 291–323, https://doi.org/10.1007/s10506-021-09294-4.

[53] Y. Razmetaeva, *The Rule of Law Crisis: Between Indefinable Values and Technological Determinism*, in UACES 2023, Themed Track The Rule of Law under scrutiny: Interdisciplinary, Theoretical and Empirical Perspectives, 2023, https://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1817778&dswid=2172.

ago. In other words, it is not a person in an empty, silent judicial chamber anymore. The imaginary judicial suite does not resemble a library in which someone chooses information independently, even if sometimes help or advice from professionals is needed. It is rather a noisy room at the crossroads of information flows, and this person is constantly but almost imperceptibly pushed to some of them. It is rather a crossroads where someone stands with a phone in their hand, constantly feeling the urge to scroll the feed, habitually using search engines, being highly influenced by opinions – widely distributed and, at first glance, supported by the public opinions, – sometimes being subtly manipulated by technologies, sometimes purposefully and successfully attacked through certain technologies.

In the context of an impact on judiciary independence, predictive analytics should also be mentioned. The development of AI technologies has brought it to a qualitatively new level. The pretended or actual predictability of judicial processes can lead to unwanted consequences, one of which being the replacement of legal certainty by an algorithmic one.

In addition, many begin to imperceptibly and excessively trust the results of certain technologies, primarily algorithms, perceiving them as objective, unbiased and infallible. However, as Mireille Hildebrandt points out, the "data-driven legal tech is not agnostic in the sense of being unbiased, objective and neutral in its prediction of case law"[54]. This misjudgement may cost us dearly as it will compromise the very essence of justice.

Those are a few of the many aspects of the rule of law undergoing digital transformation. There are other aspects, or elements, that 'feel' the full weight of the implications of the digital age. Today, as Stanley Greenstein rightly noted, "A challenge will be to determine which values to balance technology against […]

[54] M. Hildebrandt, *Algorithmic regulation and the rule of law*, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, cit.

the values enshrined in the rule of law operate as a good starting point in determining the fabric of any society"[55]. Unless we gauge our understanding of how the rule of law can work in the new technological landscape, with its significantly altered interactions, we run the risk of completely devaluing it.

At the same time, today's technologies offer innovative tools for legal research, analysis, and decision-making, enabling legal professionals to handle complex legal issues and emerging challenges efficiently. Legal research databases and AI-powered analytics allow lawyers to access vast information with unprecedented speed and accuracy. Additionally, digital platforms knowledge-sharing among them, fostering best practices. Technologies may streamline legal processes, enhance administrative efficiency, and justice accessibility. Examples include electronic case management, digital court filings, and online dispute resolution. Technologies may contribute to public audience involvement and people's wide access to legal information and services, empowering individuals to navigate legal systems and assert their rights more effectively.

These technology-mediated benefits can breathe new life into solving old problems if we rely on the value framework properly for implementing tech tools. In the digital milieu, the rule of law confronts novel exigencies as legal paradigms, sometimes antiquated, intersect with emergent technologies. This clash can still be avoided without serious casualties if an axiological and human-centric approach, rather than an algorithmic and techno-centric one, is put at the forefront.

4. Conclusions

Upholding human rights, rule of law, and democracy in the digital age necessitates concerted action from governments, civil

[55] S. Greenstein, *Preserving the rule of law in the era of artificial intelligence (AI)*, in *Artificial Intelligence and Law*, 30, 2022, 319, https://doi.org/10.1007/s10506-021-09294-4.

society organisations, and businesses. For this strategy to work, a clear step-by-step plan is necessary rather than just a set of 'beautiful words'.

Since the changes that have been taking place in the digital era are fundamental, the triad of fundamental values – human rights, democracy and the rule of law – are constantly under attack being eroded by the new technologies-centred philosophy. Having said that, a theoretical model to overcome the values crisis may be based on a two-stage approach including (1) identifying the eroded elements of the value triad, and (2) re-considering the values, working out a definitive and clear system that will work in the digital age. In any event, however, the key elements of these values must not be lost, despite the inevitable sacrifice of elements less vital.

In a nutshell, the first thing for us to do is to recognise the ongoing values crisis. That done, we need to rethink their very essence, and understand to what extent they can work as guidelines for peoples and societies. That also means re-evaluate their capacity to be applied as practical principles. If we do this, we can aspire to create a future wherein the fundamental values are flourishing.

Transparency Standards and Digital Rights

Gintarė Makauskaitė-Samuolė*

Abstract: The aim of the chapter is to review existing approaches to transparency in the European digital ecosystem. Digital rights framework adopts and adapts transparency measures of open government and also introduces new ones, combining elements from two different legal regimes. The transparency in digital services is based on the functional necessity of transparency and impact to human rights and freedoms. Nevertheless, transparency measures may need to be adjusted to cope with internal challenges like complexity and internal fragmentation.

Keywords: meaningful transparency; digital rights; digital services; transparency standards

1. Introduction

The principle of openness is rooted in primary legislation (Treaty on the European Union[1] and Treaty on the Functioning of the European Union[2]), the right to access documents (Charter of Fundamental Rights[3]) and enshrined in secondary legislation. The Court of Justice of the European Union occasionally examines openness in judicial rulings, usually in the context of limitations on access to documents held by European institutions. As summarized by Bujze, transparency in the European Union facilitates the *homo citoyen* as it contributes to democracy, assists *homo economicus*

* *Lecturer, Institute of International and European Union Law, Mykolas Romeris University Law School, Vilnius, Lithuania. E-mail: G. Makauskaite@mruni.eu*

[1] Consolidated version of the Treaty on European Union. OJ C 202 7.6.2016, p. 13.

[2] Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, p. 47–390.

[3] Charter of Fundamental Rights of the European Union. OJ C 202, 7.6.2016, p. 389–405.

by enhancing the proper functioning of the market, and serves *homo dignus* by promoting the realization of individual rights.[4]

Historically, the scope of transparency has developed exponentially, with noticeable surges sparked by significant societal, political, or technological changes[5]. As observed by Mendes, the principle of transparency in EU law remains in need of being accurately integrated through correct legal norms and proper institutional practices, or in other words, reflects a need for normative transformation.[6]

This need extends beyond the changes in the scope of transparency that stem from political shifts. Rapid digitalization and the so-called "data revolution" have changed individuals from being informed by data to being driven by data[7], if not lost in the digital domain. In response, when the EU legislators introduced the facilitation of the unrestricted flow of data in the context of the Digital Single Market, they also expanded informational rights' scope. The Digital Agenda continued this effort, which aimed to integrate the transparency principle into digital society by promoting "freedom of expression, including access to diverse, trustworthy, and transparent information."[8]

In this context, the concept of "meaningful transparency" emerged, partly based on transparency of open governance. Did it mean that the impact of the digital domain to daily lives

[4] A. Buijze, *The Six Faces of Transparency*, in *Utrecht Law Review,* 9(3), 2013, 13.

[5] A. Meijer, *Government Transparency in Historical Perspective: From the Ancient Regime to Open Data in The Netherlands,* in *International Journal of Public Administration,* 38:3, 2015, 195.

[6] J. Mendes, *The Principle of Transparency and Access to Documents in the EU: for what, for whom, and of what?* in *University of Luxembourg Law Working Paper*, 2020–004, 2020, 2.

[7] L. Taylor. *What is data justice? The case for connecting digital rights and freedoms globally*, in *Big Data & Society*, 4:2, 2017, 1.

[8] European Commission Directorate-General for Communications Networks, Content and Technology, *2030 Digital Compass: the European Way for the Digital Decade,* Publications Office of the European Union, 2021.

of individuals reached the same breadth and depth as the impact of state? Under some doctrines, current relationship of state vs. individual has modified into client-customer relationship[9]. Should governmental transparency and meaningful transparency be unified into a single standard of transparency, since they share a common material ground, even if subjects and regulatory regimes are different? To answer this question, conceptualization issues will be analyzed regarding meaningful transparency.

2. Meaningful transparency and digital rights: conceptualization

Contemporary challenges posed by the digital environment require standardized concepts within the digital rights framework that set a clear perimeter to its application scope. So, it would be complicated to implement the concept of meaningful transparency without clear answers about what transparency is, what digital rights are, and what the meaning of meaningful transparency is.

2.1. Vague definitions of transparency and digital rights

The first problem of conceptualization of meaningful transparency arises when one tries to find a uniform definition of transparency. Transparency has many faces. Transparency may be understood as a separate concept or, in the case of the instrumentalist approach, as a facilitator. It is defined as "the availability of information about an actor allowing external actors to monitor the actions and decisions of that actor." [10]It may be relational and be described as "the state that occurs if people can easily ascertain and understand the state of the world and predict how their own actions will affect that world."[11] Some narrow the transparency to organizational

[9] R. B. Denhardt, J. V. Denhardt, *The New Publice Service: Serving Rather than Steering*, in Public Administration Review, 60(6), 2000, 550.

[10] *Government Transparency in Historical Perspective: From the Ancient Regime to Open Data in The Netherlands,* cit., 191.

[11] *The Six Faces of Transparency*, cit., 4.

transparency (understood as the provider's openness about business practices and values, organizational efforts, and relationships)[12] or information transparency ("the level of availability and accessibility of market information to its participants")[13]. Consequently, in some cases, a single measure of access to information is enough to define transparency; in other cases, transparency extends to different measures and policies necessary to reach the objectives of openness.

Fluctuation of conceptual limits of transparency is also evident in transparency standards. Transparency covers different aspects in different contexts, so the standards are usually domain-specific. For example, open government standards[14] list transparency among the three critical pillars of open government, along with participation and accountability. As noted by Driessen, governmental transparency typically is about access to official documents or information, institutional transparency, openness in the decision-making, and transparency of the involvement of third-party actors.[15] However, governmental transparency standards are modifiable standards. For example, when governmental transparency is interpreted in the context of corruption, it has its modifications. Here, it is defined as the available and accessible (free) minimal public information required to deter bribery and enable public accountability in a society[16]. Some organizations applied modified transparency standards for other specific areas,

[12] R. Wang, R. Bush-Evans, E. Arden-Close, E. Bolat, J. McAlaney, S. Hodge, S. Thomas, K. Phalp, *Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications,* in *Computers in Human Behavior*, 139, 2023, 3.

[13] *Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications,* in *Computers in Human Behavior*, cit., 5.

[14] Access Info Europe, *Open Government Standards: Transparency standards*, 2023.

[15] B. Driessen, *Transparency in EU Institutional Law. A Practitioner's Handbook*, Cameron May, 2008, 5.

[16] A. Mungiu – Pippidi, *Measuring real (de facto) transparency by a new index*, In *Regulation and Governance*, 17:4, 2023, 1096.

such as lobbyism[17], public procurement[18], autonomous systems[19], content moderation[20]. Consequently, even if the benefits of transparency are unanimously recognized, the concept of transparency is multifaceted and diffused.

With the concept and protection of digital rights, it gets no better, but because of a different reason – so called "farsightedness" of the academic discourse and policymakers, when they skip the transitional stage and jump to a long-term strategy. Swift digital transformation, paired with a conceptual revision of human rights[21], is being reflected in various definitions of digital rights. For example, under the broad definition, digital rights are outlined as including human rights (both conventional and new), principles and respective guarantees.[22] Regarding the catalog of digital rights, it is incomplete. It includes conventional rights with a digital dimension (such as the right to privacy and freedom of speech and information) and novel rights (such as the right to access the Internet, the right to a digital identity, etc.)[23]. The inevitable open-endedness of the catalog of digital rights is a barrier to define the role of transparency in it. Internal

[17] Organization for Economic Cooperation and Development, Recommendation of the Council on Principles for Transparency and Integrity in Lobbying, OECD/LEGAL/0379, OECD, 2023.

[18] Organisation for Economic Co-operation and Development, *Compendium of Good Practices for Integrity in Public Procurement*, GOV/PGC/ETH(2014)2/REV1, OECD, 2015.

[19] A. F. T. Winfield, S. Booth, L. A. Dennis, T. Agawa, H. Hastie, N. Jacobs, R. I. Muttram, J. I. Olszewska, F. Rayabiyazdi, A. Theodorou, M. A. Underwood, R. H. Wortham, E. Watson, *IEEE P7001: A Proposed Standard on Transparency,* in *Frontiers in Robotics and AI*, 8, 2021.

[20] The Santa Clara Principles: On Transparency and Accountability in Content Moderation, 2018.

[21] Y. Razmetaeva, Y. Barabash, D. Lukianov, *The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice*, in *Access to Justice in Eastern Europe*, 2022, 43.

[22] K. I. Bieliakov, O. O. Tykhomyrov, L. V. Radovetska, O. V. Kostenko, *Digital rights in the human rights system*, in *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations*, 10, 2023, 191.

[23] *Digital rights in the human rights system*, cit., 193.

categorization of rights – to those with a digital dimension and who are "born digital" – implies a somewhat different position of each category and a slightly different effect of transparency, even if equivalent protection is accentuated in them. The difference stems from the choices of policymakers, but these choices are quick, discretionary, and not uniform. Regulatory efforts concerning digital rights lag behind the academic discourse, showing considerably more restraint and less maturity. In response to digital transformation, some countries chose to develop broad digital policy frameworks, while others began exploring and legitimizing specific digital rights (for example, the right of access to the Internet in France, Finland, and Estonia[24], right to disconnect in Germany), some prioritized protecting rights online in the same way they are protected offline[25].

A rush to a long-term vision without establishing essential clarity in tactics is also characteristic at a regional level. Declarations of international and civil society organizations, such as the EDRI Charter for Digital Rights[26], the Lisbon Declaration[27], European Declaration on Digital Rights and Principles for the Digital Decade[28], shaped the European digital strategy. Legislators did not create standards in these declarations to reiterate the equivalent protection of "offline" and "online" human rights. Regional policymakers acted with an intent to shape future

[24] C. Cocito, P. De Hert, *The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights)*, In *Computer Law and Security Review*, 50, 2023, 9.

[25] Organization for Economic Co-operation and Development, *Rights in the digital age: Challenges and ways forward*, in *OECD Digital Economy Papers*, 347, 2022, OECD Publishing, Paris, 14–15.

[26] European Digital Rights, *The Charter of Digital Rights*, in *The EDRI papers*, 2014.

[27] Portuguese Presidency of the Council of the European Union, *Lisbon Declaration – Digital Democracy with a Purpose*, 2022, Retrieved from: https://www. lisbondeclaration.eu/

[28] European Declaration on Digital Rights and Principles, 2022. Available at: https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

digital strategies[29], but tactical – near future – changes were left to the discretion of national policymakers. An apparent digital divide through uneven digital progress in the EU Member States is troublesome, as basics of the digital world, such as digital empowerment, enterprise digitalization, and broadband access, were enlisted as the most pressing needs.[30] Over the past decade, there has been a consistent decline in freedom of expression, even in states that are recognized as leaders in digital transformation [31]. Therefore, one should expect the future progress of the digital rights framework to be complicated.

2.2. Vague meaning of meaningful transparency in the European Union

Concepts of transparency and digital rights are only some of the indefinite; meaningful transparency is as ambiguous as they are. The purpose and scope of the transparency measures define the "meaning" in it. Regarding the purpose, transparency is usually a response to situations characterized by trust issues; in the past, the demand for transparency was often fueled by distrust toward previous regimes and governing elites and was associated with state modernization.[32] The EU is no exception. Trustworthiness is a crucial milestone in the competitive digital ecosystem designed by the EU.[33] It leads to the question of who is distrusted and with

[29] *The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights)*, cit., 5.

[30] H. Pinto, C. Nogueira, G. Vieira, *Digitalization landscape in the European Union: Statistical insights for a Digital Transformation*, in *European Public and Social Innovation Review*, 8, 2023, 34–35.

[31] United Nations Development Programme, *The impact of digital technology on human rights in Europe and Central Asia: Trends and challenges related to data protection, artificial intelligence, and other digital technology issues*, United Nations Development Programme, Istanbul, 2023, 5.

[32] *Government Transparency in Historical Perspective: From the Ancient Regime to Open Data in The Netherlands,* cit., 195–198.

[33] K. Prifti, J. Krijger, T. Thuis, E. Stamhuis, *From Bilateral to Ecosystemic Transparency: Aligning GDPR's Transparency Obligations with the European Digital Ecosystem of Trust*.

whom. Art. 3a of Digital Decade Decision accentuates the universal scope of transparency addressees ("accessible to all, everywhere in the Union"[34]). In the communication on shaping Europe's digital future[35], the Commission emphasizes that greater transparency is necessary to enable the activated individuals to act as Buijze's homo dignus ("helping consumers take greater control and responsibility for their data and identity"). It follows that "meaningfulness" is an inherent component of transparency; it must correspond to everyone's needs to build trust and that distrust is a reason for being passive.

The early conclusion is not supported by the texts of declarations in the digital rights field that fail to offer a clear answer to the purpose and scope of meaningful transparency. However, they have statements on the importance of transparency in particular areas. For example, transparency of information access, data protection, and remote participation are highlighted in the EDRI Charter for Digital Rights[36]. Transparent technology use in the workplace, algorithms and artificial intelligence, and transparent information on online services are mentioned in the European Declaration on Digital Rights and Principles for the Digital Decade[37]. So, declarations "sell the idea" of transparency, and the requirement of "meaningfulness" comes after.

In S. Kuhlmann, F. De Gregorio, M. Fertmann, H. Ofterdinger, A. Sefkow (eds.), *Transparency or Opacity: A Legal Analysis of the Organization of Information in the Digital World*, Nomos, Baden-Baden, 2023, 115.

[34] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. PE/50/2022/REV/1. OJ L 323, 19.12.2022, p. 4–26.

[35] European Commission, *Shaping Europe's Digital Future,* Publications Office of the European Union, Luxembourg, 2020.

[36] EDRI, The Charter of Digital Rights, 2014. Available at: https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

[37] European Declaration on Digital Rights and Principles, 2022. Available at: https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

The silent component of the meaningfulness of transparency is evident in the case of informational rights. For example, an individual has informational rights, including right to a personal file and explainability, under the General Data Protection Regulation (GDPR)[38]. Other acts related to digital acquis – Platform to Business Regulation (P2B), the Unfair Commercial Practices Directive (UCPD), and the Consumer Rights Directive (CRD) are targeting platform users in case of rankings.[39] Businesses were provided with limited informational rights, too, like facilitating the access or exchange of data in case of transport means and financial data.[40] and so on. In contrast, Public Sector Information Re-Use Directive[41] has broad objectives of promoting competition and transparency in the information market; the scope of information to be accessible is very broad. As the scope and conditions of informational rights are very different, meaningfulness is then adaptable to the context. The risk here lies not in the various meanings but in how these meanings are aligned together.

A problem of incomplete coordination among regulatory measures or justification of their meaningfulness is grounded. For example, addressees of informational duties regarding distance and off-premises contracts in the Consumer Rights Directive[42]

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88.

[39] C. Busch. *From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation*, In S. Genovesi, K. Kaesling, S. Robbins, *Recommender Systems: Legal and Ethical Issues*, 40, 2023, 39.

[40] *Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market?* Cit., 334.

[41] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

[42] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/

differ compared to addressees of informational duties regarding commercial practices in the Unfair Commercial Practices Directive[43] or addressees of informational duties regarding digital services or platform to business, even if the functionality – recommender system – is the same.[44]

Challenges to implementing meaningful transparency standards are intrinsic in digital technology, market behavior, and the European Union's strategy. From a technological perspective, data sharing is critical for a modern digital ecosystem. Therefore, transparency must go aside the data, both horizontally and vertically. And not only transparency but also responsibility. Prifiti et al. note that "it is much more relevant to assess data infrastructures, institutions, and mechanisms."[45] and claim for responsibilities to be redistributed among multiple parties. Transparency obligations must bind users, businesses, institutions, and civil society.[46]

From a business perspective, previous self-regulation of the digital market left its footprint upon the practices of digital businesses. In economic-incentive business models centered around user engagement, human rights compliance costs are not welcome. The impact is transnational because Big Tech companies dominate the digital services market in Europe.

EEC and Directive 97/7/EC of the European Parliament and of the Council. OJ L 304, 22.11.2011, p. 64–88.

[43] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'). OJ L 149, 11.6.2005, p. 22–39.

[44] *From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation*, cit., 41.

[45] *From Bilateral to Ecosystemic Transparency: Aligning GDPR's Transparency Obligations with the European Digital Ecosystem of Trust*, cit., 130.

[46] *From Bilateral to Ecosystemic Transparency: Aligning GDPR's Transparency Obligations with the European Digital Ecosystem of Trust*, cit., 130.

From a strategic perspective of the EU, extraterritorial application of EU's *digital acquis* is one of the milestones of future strategy. For example, clauses on transparency within the Digital Services Act (further also referred as DSA)[47] apply to digital services provided to individuals or entities established or located within the European Union. Challenges related to extraterritorial application, such as multilingualism, multiculturalism, uneven digital development, and the digital divide, suggest that current standards may need to be modified to tackle these issues.

Besides, after reaching digital targets for 2030 of the second Digital Decade, the EU is planning to regulate the next technological transition, including immersive technologies, development and use of virtual worlds and Web 4.0[48]. Today's basic digital development level is planned to be lifted to a much higher level. Current digital technologies have already created new ways of exercising fundamental rights and freedoms, and in some cases, novel digital human rights emerged. The same trend is suggested to continue in the future.

Policymakers are currently in the process of reinventing meaningful transparency standards to regulate the new digital reality. Elements of the standards are borrowed from existing national regulations on transparency, redress, and data access; new concepts (such as trusted flaggers) were suggested by academia and civil society[49]. But are the meaningful transparency standards, currently integrated into the digital acquis of the EU, capable to help reaching the objectives of the Digital Agenda?

[47] 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). PE/30/2022/REV/1. OJ L 277, 27.10.2022, p. 1–102.

[48] European Commission, *An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition*, COM(2023) 442/final, Strasbourg, 2023.

[49] D. Holznagel, *Art. 21 DSA – what to expect*, in *CR-online.de Blog*, 2023, retrieved from: https://www.cr-online.de/blog/2023/09/21/art-21-dsa-what-to-expect/

The newest component of EU digital acquis – the Digital Services Act (DSA) was chosen for a more detailed analysis. Meaningful transparency standards of digital services (based on the Digital Services Act) are compared to open government standards[50]. and analyzed considering the objectives of the EU Digital Agenda[51].

3. Meaningful transparency standards in the Digital Services Act

3.1. Transparency by rules

In governmental transparency standards, "transparency by rules" is part of the rule of law and legal certainty. Transparency by rules requires that laws and decisions are public, specific, and straightforward.

In digital services, "transparency by rules" primarily safeguards a different objective – predictability and equality of parties. "Rules" include terms and conditions, policies, procedures, instructions, other documentation, and information necessary to know before engaging with or using a given service or product. Privacy and cookie policies, content policies, sustainability policies, platform or payment policies, codes of conduct, community guidelines, and template agreements fall into the scope of rules.

Three groups of transparency obligations are covered by "rules": the right of individuals to get access to information about the conduct of a provider, access to information about the rights that individuals have about the conduct, and the right to intelligible information on the manner (the "how") of conduct.[52] Meaningfulness for an individual is an implied delimitator of the

[50] Access Info Europe, *Open Government Standards: Transparency standards*, 2023.

[51] European Commission, Directorate-General for Communication, Digital agenda for Europe – Rebooting Europe's economy, Publications Office, 2014, https://data.europa.eu/doi/10.2775/41229

[52] *From Bilateral to Ecosystemic Transparency: Aligning GDPR's Transparency Obligations with the European Digital Ecosystem of Trust*, cit., 119.

scope of rules to be published. Criterium of meaningfulness is used to preserve the equality of parties and protect from informational noise. It is reminiscent of governmental practices of some Member States to publish "meaningful" (and not all) case law that attempts to balance the administrative burden of authorities with the public right to know. In such cases, clear criteria of meaningfulness, as well as safeguards against the personal preferences of decision-makers, must be in place to protect from the arbitrary limitation of the scope of information.

Transparency of terms and conditions is a joint obligation, binding all digital service providers under the Digital Services Act. The reason why terms and conditions must be transparent lies in the disturbed relationship between service recipients and providers, where providers may have significant bargaining power compared to individual users who are pushed to accept their rules[53]. So, the way platforms enforce their terms and conditions is governed in them, and, importantly, a new obligation to consider users' "fundamental rights" under the EU Charter with "due regard" is introduced there. The latter, interestingly, is typical of vertical relationships between state vs. citizen.

Vertical relationships and state-similar obligations (decision-making, complaints, procedures, and safeguards) are embodied in the content of terms and conditions. It is required that the content should contain the grounds to restrict the use of the service, in particular details regarding all policies employed for content moderation, together with procedures for algorithmic decision-making and human review, an internal complaint mechanism, and easily accessible information on the right to terminate the use of the service. It must be noted that requirements for terms and conditions in the DSA are different for all digital acquis. An

[53] *Using Terms and Conditions to Apply Fundamental Rights to Content Moderation*, cit., 883.

example would be the instructions for high-risk AI systems, which are somewhat comparable to medication leaflets: the information is significantly more detailed there. The AI instructions should outline risks, trials, and usage details.

If the terms and conditions are equal to an agreement between parties (one party weaker than the other), what about the situation when terms and conditions change? In digital services, intermediary service providers are required to notify recipients of the service about any significant – not all – changes to the terms and conditions. Significance is measured through the impact of changes on the recipient when using the service. In comparison, governmental transparency does not create a duty of notification of laws based on the principle *ignorantia juris non excusat*. The public watchdog partly accomplishes the notification in the latter case – media.

Does regulation of terms and conditions in digital services enhance transparency and advance the objective of empowering citizens? Agreeing to terms and conditions still constitutes a binding contract.[54]. Adjusting the content to user comprehension should restore the balance between the rights of the involved parties. But it is not a secret that terms and conditions are some of the least-read texts on the Internet[55]. So, a positive outcome can be expected only if "transparency by rules" goes together with "transparency by design" and organizational changes related to assessing the impact on human rights.

3.2. Transparency by default

"Transparency by default" is established in open government principles 1–4[56]. Explicit recognition and adherence to maximum

[54] P. Leersen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in *Computer Law & Security Review*, 48(1), 2023, 6.

[55] *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, cit., 6.

[56] Access Info Europe, *Open Government Standards: Transparency standards*, 2023.

disclosure are vital for governmental transparency. Consequently, governments should recognize the fundamental right of the public to access information, preferably at the constitutional level. The information must be published proactively and made available reactively in response to requests.

In the eyes of legislators, digital services are different from governmental services. The principle of maximum disclosure is not expressly recognized in the Digital Services Act, and providers are not required to amend their policies accordingly. Instead, many clues demonstrate that only targeted, functional transparency is established, based on the functional necessity to know and impact to human rights and freedoms. Digital providers are not required to take on a duty to act as openly as possible.

Besides, there is no general requirement to interpret the exceptions to disclosure strictly and closed-ended. When in doubt about disclosing specific information, one is not required to favor disclosure, with one exception. An explicit override of public interest of transparency is seen in the case of researchers' access to data. Refusal to grant access to data essential for specific research objectives should not be solely based on the commercial interests of data providers.

Among material grounds to limit transparency, confidentiality is expressly listed in the preamble of the Digital Services Act; due to it, the Commission's decisions may be disclosed not in full but to an extent that allows the "addressee of the decision to understand the facts and considerations that led up to the decision"[57]. Transparency reports are a bit closer to the principle of maximum disclosure with a determinate list of exceptions to limit disclosure (potential disclosure of confidential information of provider or recipients of the service, potential significant vulnerabilities for

[57] P. 146 of the Preamble of the Digital Services Act, cit.

the security of digital service, potentially undermined public security, or harm to recipients). In enforcement proceedings, only professional secrecy is cited as a reason to restrict transparency. Access to data for researchers must be ensured without prejudice to the protection of business know-how and trade secrets.

3.3. Transparency by scope

"Transparency by scope" in the context of open government means that all kinds of official information should be public, irrespective of their form and holders. The terms "public body" and information should be interpreted as widely as possible, including all bodies performing public functions and operating with public funds. Lately, it was extended to cover private bodies holding information that relates to or is necessary to protect human rights.

In the Digital Services Act, not all information society services are covered, just intermediary services, and the scope of transparency obligations is not uniform. Transparency obligations differ based on service type and provider audience size. Three transparency "layers" are implemented in the DSA: a layer of standard requirements, activity-specific requirements, and a layer of transparency obligations for the largest digital service providers (very large online platforms and very large online search engines). Therefore, what matters is the capacity of actions to affect fundamental rights and freedoms on a significant scale and depth, which correlates with the extent of transparency obligations. The pattern of risk scalability evident in the DSA corresponds to the proportionate risk-based approach of the AI systems in the AI Act. AI systems are also subject to different transparency requirements based on their risk level, which is calculated by the use and potential impact on fundamental rights or freedoms.

As mentioned before, only specific, predefined information will be provided, based on necessity and meaningfulness to know (the principle is reiterated in the GDPR, P2B Regulation, etc.)

Another dimension of transparency by scope concerns the addressees of openness. Regarding governmental transparency, the right to access official information is universal and extends to all members of the public. Individuals who seek access to official information are only required to provide motives for their request if they want to access a personal file or under other circumstances that require more confidentiality.

In intermediary services, the scope of transparency is customized to the audience it serves. The target audience comprises the segments of recipients of the service, supervisory institutions, civil society, and academia. Information is customized to each segment; the target audience must be able to understand and use that information. Legislators of the DSA had in mind apparently that general access to information in open government was expected to activate all segments but failed; civil society remained passive, but expert users – researchers and companies were active. [58]. So, customization of the scope of information in the DSA was a pivotal attempt to activate the audience differently and not to repeat mistakes. The success of this experiment, however, depends on the genuine will of providers to do their best when providing the information and the target audience's natural interest in utilizing the information.

3.4. Transparency by limitations

In governmental transparency, refusals to disclose information are subject to procedural safeguards – individually performed harm tests and public interest override tests. They contain

[58] *The Principle of Transparency and Access to Documents in the EU: for what, for whom, and of what? cit.*, 12.

proportionality, legitimacy, and purpose assessments that were occasionally interpreted in the case law of international courts. The list of limitation grounds is exhaustive; limitations are to be interpreted narrowly.

In DSA, limitations are double-sided: they may limit the rights and interests of others, such as the free flow of information in case of content moderation, and may also restrict the provider's rights and interests, such as an obligation to respect human rights. A universal list of restrictions is not defined; the legislator highlights certain rights and interests that are especially important for striking a proper balance in a specific situation. However, these rights and interests are only some of the ones to be balanced.

An example of this "intentional silence" is with intermediary service providers and human rights assessments. Intermediary service providers must diligently, objectively, and proportionately assess the "rights and legitimate interests of all parties involved"[59] when implementing restrictions. For assessment, the notion of human rights is not limited to the EU Charter of Fundamental Rights and includes other rights and legitimate interests. Also, it needs to be clarified how much of a direct link to human rights should be, i.e., if the balancing act requires strict human rights *stricto sensu* or *sensu lato*. In the first case, rights and interests would be limited by the directly involved parties of the relationship; in the second case, the human rights assessment would include not only individual rights but societal rights, also[60]. Due diligence obligations of the intermediaries suggest that the broader public was in mind of the legislators, but legislators chose to be intentionally flexible, leaving a space to maneuver. Nonetheless, there are doubts if such

[59] Art. 14 of the Digital Services Act, cit.

[60] N. Appelman, J. P. Quintais, R. Fahy, *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?, in DSA Observatory,* 2021.

vagueness of the scope of this obligation leads to the later effect of this rule.[61].

The provider's active role – seeking solutions to act in compliance, not circumvention of human rights obligations – is implied. To reinforce the active role, it is established that even if core principles of liability regime, prohibition of general monitoring, and internal market clause delimitate providers' freedom to choose their means to achieve the goal, they cannot be understood as a constraining factor regarding assessments.

Assessment tests on limitations are to be performed not for all provider activity but for the most risk-prone areas – in the context of content moderation, access to data, and systemic risks. But are they comparable to assessment tests in governmental transparency? Or do they establish a custom standard of assessment tests in digital services? Alternatively, are they context-dependent?

Compared to governmental transparency, the first difference is the external scope of application of assessment tests (both for ingoing and outgoing information). Besides, it is evident that assessment tests require modification internally and cannot be transposed as such into digital services. In content moderation, circumstances differ from those when accessing official information. In content moderation, providers are not withholding their information; they are interfering with the circulation of information they host. Consequently, it is essential to check and test the enforcement procedures of content moderation, the discretion exercised by providers, and the existing safeguards to prevent undue restriction of content.

This obligation of review is owed by supervisory institutions, auditors, and the public (via disclosure of rules and trusted flaggers). And the complicity of having a shared responsibility does

[61] *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions? cit.*

not end here. Transparency in content moderation is not limited to the performance of assessment tests; the obligation of assessment of risks is a single part of the extensive content moderation transparency framework. The content moderation transparency rules require publishing the provider's content moderation standards and disclosing policies, procedures, measures, and tools used for content moderation, algorithmic decision-making, and human review. It also entails disclosing the rules of procedure for their internal complaint handling system in their terms and conditions, conducting transparency reporting, risk assessments, and audits, and providing data to a Commission's transparency database. Moreover, it entails regulating the content moderation process itself and allowing involved parties to participate in it (by trusted flaggers), as well as monitoring how their services are used to disseminate or amplify misleading or deceptive content, including disinformation[62]. The notice and action framework and trusted flaggers seek to tackle the issue of overly blocked content reported as illegal. A significant challenge for the provider is to fulfill these responsibilities while also adhering to the principle of not being able to monitor content generally or engage in fact-finding activities.

Can content moderation, as regulated in the DSA, effectively address the issue of transparency? At first sight, it is undeniable that the framework of transparency measures is innovative. Not only is it systemic and self-supporting, but it also involves a variety of stakeholders.

However, challenges exist. From the perspective of limitations, it must be borne in mind that the performance of procedural tests on limitations is delegated to the provider's lay employees (editors, moderators). They cannot be compared to professional lawyers or

[62] p. 84 of the Digital Services Act, cit.

civil servants (as in the case of governmental transparency) or have time to thoroughly seek a balance of interests. Material grounds to restrict the content are not limited to illegality (the concept varies worldwide) but include incompatibility with providers' terms and conditions. The common challenge with terms and conditions is that they are often updated; they are drafted loosely with open-ended terms and definitions.

For evaluation of de facto transparency, Article 24 (5) of the DSA requires providers of online platforms to send all their statements of reasons to the Commission's DSA Transparency Database, which is publicly accessible and machine-readable. With 73 % of automated decisions and top restriction of visibility[63] The Commission's DSA Transparency Database is already pointing to potential risks. Safeguards are needed from the impact of the mismatch between the profile of human reviewers and the context reviewed, which is too vague.

The DSA regulates visibility reduction, such as shadow banning, reranking, and demonetization. Proving these visibility reduction measures can be challenging due to inbuilt coding errors, personalization, and dynamically shifting results in a result list.[64]. Moreover, they are detected ex-post, with ex-ante prevention scarcely addressed in the DSA. The impact to human rights protection would be improved if transparency of content moderation would include ex-ante transparency measures.

DSA provides exemptions for content moderation actions that target "deceptive high-volume commercial content," including bots, creation of fake accounts, and commercial spam messages. Content that is not of commercial nature, such as

[63] European Commission, DSA Transparency Database, available at: https://transparency.dsa.ec.europa.eu/, last accessed 18 February 2024.

[64] *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, cit., 7.

propaganda, is not covered. The exemption is narrowed to "deceptive," and given that most of the statements of reasons are automated, verification of deception creates a problem. To do this, providers must find a way to verify deception without general monitoring, active "fact-finding," or proactive illegal content measures. Since there is no requirement to "engage in excessive or costly online fact-finding exercises or to carry out disproportionate verifications on the spot"[65] this could result in monitoring for overtly commercial content (automatic match of specific keywords) rather than discreetly examining all content. DSA, differently from P2B Regulation, does not allow to ignore the duty to provide statement of reasons for users based on their repetitive behavior[66]. It establishes a different, higher transparency burden on DSA providers than business users in P2B Regulation. Indications of an implicit principle favoring maximum disclosure could be apparent in this exception.

Regarding the data access for researchers, the research objectives limit the scope of the data. It should pass the necessity and proportionality and purpose test ("necessary for, and proportionate to, the purposes of their research and that the expected results of that research will contribute to the purposes," Art. 40 of the DSA). DSA mentions content engagement analytics and real-time data but is not limited to these. Importantly, reflections of maximum disclosure can be seen, as there are only two grounds to refuse to provide data (no access or significant vulnerabilities in the security of service or the protection of confidential information, in particular, trade secrets, Art. 40 of the DSA) and providers are required to offer alternatives. The cost of creating the proper infrastructure of access or adaptation of

[65] P. 73 of the Preamble of Digital Services Act, cit.

[66] *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, cit., 7.

current access regimes to meet technical requirements on security and sensitivity and meaningful use of the data is not mentioned among exceptions to provide data.

The transparency duty on data access is also subject to an interest balance test where the rights and interests of providers, recipients, and any other concerned parties would be weighed. Protection of commercial interests, as one of the typical exceptions to provide public information, is explicitly not outweighing the interest of the researchers; the researchers themselves must prove that they are independent of commercial interests.

Under the DSA, the interest balance test is to be done by researchers or their organizations and assessed by Digital Service Coordinators. The public interest is required to publish the research results (they should pass the same interest balance test) publicly and free of charge.

The most professional and complete assessment of limitations is to be performed in the context of systemic risks by very large online platforms and very large online search engines. Severity and probability must be considered. Four types of systemic risks are enumerated in the DSA, but the list is not closed or limited to the EU Charter of Fundamental Rights or EU law. DSA in the paragraph 47 of the Preamble refers to relevant international standards for protecting human rights, such as the United Nations Guiding Principles on Business and Human Rights. Freedom of information and pluralism are highlighted as particularly important. The providers must mitigate risks to fundamental rights.

However, the regulation of systemic risk assessment could be better. It lacks clarity on what systemic risk is, what is illegal, what the scope is, and how to measure the impact. Existing human rights risk assessment methodologies may be adapted for this reason, but creating and adopting a methodology takes time. The ambitious intention needs to match the preparedness and

willingness of providers to complete such assessments and the supervisor's capability to review them.

3.5. Transparency by data

In governmental transparency, "transparency by data" corresponds to open government principles No. 6–7. It requires information to be delivered electronically and in an open format, and bodies are obliged to compile information necessary for public participation and accountability regularly. Information must be, in general, provided free of charge and free for reuse.

Reflections on the principle of "transparency by data" are more elaborated in the regulation of digital services. Transparency of access to data to vetted researchers is a new transparency duty for very large online platforms and very large online search engines (further referred as VLOSEs). It supplements the access to data that supervisory authorities and auditors have when conducting their inspections and evaluations. The logic is facilitating researchers affiliated with a research organization to conduct independent investigations and offer a secondary, objective perspective on providers' innovations regarding systemic risks. A severe flaw of access to data is that it enables evaluations after the fact and may only be suitable for prevention if real-time data is provided.

On the other hand, researchers' access to data creates an extensive administrative burden for providers. The responsibilities of providers and researchers are not expressed clearly enough. For example, the number of requests, the number of researchers, or the depth of data is not limited. The timeframe for approving researchers as vetted and granting access to data is governed by the vague term "without undue delay." Specific criteria for selecting researchers have yet to be defined. Access is granted to individual researchers. Based on this, there is a presumption that researchers should focus on quickly reachable, "low-hanging

fruits" of research and be able to communicate the results to the public and media.

Technical standards for data access based on Art. 44 of DSA will be approved shortly, with real-time data accessible if possible. Standards are meant to make a broader impact on the EU market, as the standards will be updated publicly and easily accessible. For now, their content needs to be clarified. The publicized intention of the researchers to get experimental data and copy of data scraped from the web is doubtful. Experimental data allows researchers to understand the logic behind algorithms. However, harm to the provider due to the sensitivity of data and the presence of trade secrets would overrule the needs of researchers. At the same time, web-scraped data enables the verification and validation of the quality of data services provided in compliance with the DSA. Again, web scraping may negatively impact the stability and security of digital services, so it is highly doubtful if these segments will be included in the scope of technical standards.

Another potential challenge lies in the conflict between the clauses of the DSA and GDPR. Academic freedom of expression and scientific research have different scopes of exemptions by the GDPR[67], are likely to require further clarifications in the case of DSA's regulated access to data on the balance of providers' and researchers' duties. Providers and researchers are responsible for data protection when providing access or conducting and publishing research. Not having the recipients' consent most likely will not be an excellent excuse to give data; for these reasons, "legal obligation" under the GDPR would fit the regular use case.

The objectives of the research – to address the systemic risks for the public – imply a constant push for very large online

[67] The European Data Protection Supervisor, *A Preliminary Opinion on data protection and scientific research,* EDPS, 2020, 10.

platforms (further also referred as VLOPs) and very large online search engines (further also referred as VLOSEs) to work better when coping with these risks. Besides, VLOPs and VLOSEs are seen not only as generators of systemic risks; if they were, third-party audits and conventional supervisory powers of authorities would possibly be enough. They are also regarded as valuable think tanks holding more knowledge and talent than the rest of society and are forcefully compelled to share it. So, the need to strengthen transparency through balancing tests, data access, and public research is driven by the twofold aim of mitigating risks and directing innovation towards non-commercial domains. Transparency means that the protection of providers' "commercial interests" is shrinking, and openness is more comprehensive than open government.

3.6. Transparency by language

"Transparency by language" corresponds to open government principle No. 7. It requires that information necessary for public participation and accountability be clear, comprehensive, and comprehensible.

In the DSA, clarity of language serves to manage user expectations. Complex legal or technical jargon, open-ended terms, and vague drafting of restrictions should not be used.

The benchmark for the intelligibility of the language of terms and conditions in the DSA is higher than in the GDPR and AI Act. While GDPR requires a "clear and plain" language, DSA also necessitates intelligible, user-friendly, and unambiguous language for the terms and conditions. However, information about recommender systems in terms and conditions must be "plain and intelligible." When contrasted with high-risk AI systems, their transparency benchmark in instructions of use of AI system is constructed as

with a "certain degree of transparency"[68], allowing users to interpret the system output and utilize it effectively. However, in practice, "concise, complete, correct and clear information that is relevant, accessible and comprehensible to users" would demand higher effort than digital services.

For DSA, complete clarity for any user category is required, leaving no room for interpretation. Interestingly, if the digital service is primarily directed at minors or is predominantly used by them, it must explain conditions or restrictions "in a way that minors can understand," but only very large platforms and search engines have a duty of translation to the user's language. The high standard posed for the clarity of information corresponds to the standard of the "average user" that uses the digital service.

Nevertheless, it is regrettable that the requirement for "transparency by language" was not explicitly expanded to be applied to the entire content of terms and conditions and other documentation. Besides, only very large online platforms and very large online search engines must provide a summary of terms and conditions "in clear and unambiguous language."

Comprehensibility and easy access are the focus of information provided about the advertisements, as it must be presented in a "clear, concise and unambiguous manner and in real-time" (in Art. 26 of DSA) and include "meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters." (in Art. 26 of the DSA) The average recipient of the service is provided with individualized information necessary to understand when and on whose behalf the advertisement is

[68] European Commission, *Proposal for a Regulation of the European Parliament and of the Council, laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts,* COM(2021) 206 final.

presented (see p. 68 of the Preamble of the DSA). Therefore, the higher standard of the average user as "reasonably well-informed and reasonably observant and circumspect" (see p. 18 of the Preamble of Unfair Commercial Practices Directive) as in Unfair Commercial Practices Directive is not applicable in DSA[69].

3.7. Transparency by design

"Transparency by design" relates somewhat to the proactive publication standard of open government but goes beyond that. Public bodies must make "every effort to ensure easy, prompt, effective and practical access to such information."

The concept of transparency by design is often used as a synonym for interpretability, which demonstrates "the degree to which a human can understand the decision-making process of a model examining its internal structure."[70] Interpretability should be distinguished from explainability, which uses "transparency by language" to explain the output or result but may fail to interpret "how it was made" (as deep learning AI models). [71] In the DSA, those two approaches are broadly brought together by requiring the provisioning of meaningful explanations next to ads of the logic used to that end, including when this is based on profiling. Thus, the requirement is result – and not the process – oriented, where the result is the state of understanding.

The impact of design on decision-making processes has already been validated through the concept of "privacy by design," codified in the General Data Protection Regulation (GDPR). "Transparency by design," set in both the AI Act and the Digital Services Act (DSA), changes routine practices of system engineering and design.

[69] *From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation*, cit., 39.

[70] *The role of explainable AI in the context of the AI Act*, cit., 1142.

[71] *The role of explainable AI in the context of the AI Act*, cit.,1143.

Is the "transparency by design" standard different in digital services and in AI systems? The answer depends on who the user is. In AI systems, the user is educated. AI users have the function of human oversight of the AI system. This function demands a higher transparency standard, where design, development, and human-machine interface tools are adequate for the control of the AI[72]. In the case of digital services, the user or recipient is a layperson. The design of the system's interface is much more visible for the lay recipient of digital services. That implies more transparency duties: from a duty to mark advertising to the prohibition of dark patterns in the organization, design, or operation of the system (see Art.25 of DSA), to prepare an interface for the traders to demonstrate their compliance, to adapt the interface to minors and improve accessibility. In DSA, the marking of ads must be optimized for an average service recipient and adapted to the individual service's online interface. Therefore, visual transparency requires the design to be fair, accessible, and tailored. In some cases, it is expressly timely. For example, the obligation to disclose trader information is ex-ante (before allowing those traders to sell products on the platform) and information on entities behind the ads.

Commissions' obligation to issue standards on design and providers' duty to address systemic risks posed by design are separate from each other, so adherence to design standards may not remove systemic risks by default. Design must be free from evident systemic risks at the launch (with the help of compliance function within the organization), but those that were not visible or became visible after the change of external circumstances should fall into the scope of systemic risk analysis (post-factum). The design developers must balance "healthy engaging" vs."addictive"

[72] European Commission, *Proposal for a Regulation of the European Parliament and of the Council, laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts,* COM(2021) 206 final.

and put extra safeguards for minors. That would mean that the developers working for a private entity should be able to act impartially and have expert knowledge. Therefore, systemic risks may be evident in the long run.

3.8. Transparency by the numbers

Transparency by the numbers, term to describe quantifiable metrics, provide an objective view of compliance status, ensuring data comparability within the framework of the DSA. Transparency by the numbers is an innovative measure not mentioned in the principles of open government.

Fields where metrics are essential include trusted flaggers reports, data access for researchers, and data submitted to public compliance databases, such as for the statements of reasons and advertisements, risk assessment procedures, and audits. Objective communication by the numbers empowers stakeholders to apply coordinated pressure on service providers or at least enhance their understanding of how digital services operate.

With transparency reporting obligation binding upon intermediary services, it is intended to inform the public at large on the content moderation practices of the service provider, to empower users to make informed choices and to increase public pressure on platforms and governments (when they order content removal). By Article 15 of the DSA, all intermediary services (except for micro and small enterprises) are mandated to release transparency reports on content moderation at least once annually. These transparency reports must be objectively justified in terms of numbers. Providers are required to center on details regarding orders received from authorities of Member States, notices submitted through the notice and action mechanism, content moderation actions taken autonomously, and complaints received via the internal complaint-handling system. The legislator has not yet provided the standards applicable to these

reports, and it has already ended in the incomparability of the first transparency reports and a compromised value to transparency[73]. In the (temporary) absence of regulator's guidance, civil society recommendations, such as Santa Clara Principles 2.0[74], were not largely followed[75].

Can transparency by the numbers effectively enhance transparency? Informed decision-making necessitates precise and timely data. Would the data in transparency reporting have such qualities? The researchers noticed the trend of "washing" the numbers within the transparency reports.[76] For individuals, annual transparency reports should be shorter and simpler to assist in daily decision-making, so a comparative transparency index (including a cumulative one from the group of companies) in a visual form would be more beneficial. Given the unsatisfactory level of digital skills of individuals, other proactive measures should protect them from "transparency washing" as well, but that, as elaborated in academic literature, would require refocusing on stricter regulation of technology companies and not "creating more private "transparency" principles and initiatives" [77].

3.9. Transparency by choice

Transparency by choice is another innovation that is not present in open government principles and is characteristic of the

[73] A. Urman, M. Makhortykh, *How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms,* in *Telecommunications Policy*, 47:3, 2023, 13.

[74] The Santa Clara Principles: On Transparency and Accountability in Content Moderation, 2018.

[75] The Santa Clara Principles: On Transparency and Accountability in Content Moderation, 2018.

[76] A. Reid, E, Ringel, S. M. Pendleton, *Transparency reports as CSR reports: motives, stakeholders, and strategies*, in *Social Responsibility Journal*, 20:1, 2024, 84.

[77] M. Zalnieriute, *"Transparency Washing" in the Digital Age: A Corporate Agenda of Procedural Fetishism*, in *Critical Analysis of Law*, 8:1, 2021, 153.

DSA. The DSA shows an attempt to establish transparency through neutral choice integrated into recommender systems. The neutral choice helps minimize the biased ranking and optimize ranking.[78] Because of the choice, service recipients are informed about their option to select or modify their ranking options and have the main parameters, significant criteria, and reasons for their relative importance explained to them. In addition, providers of very large online platforms and online search engines should consistently ensure alternative options are not based on profiling.

Default choices are regulated in the context of manipulation, with complicated changes of default settings and protection of minors, where default choice must guarantee high privacy, safety, and security.

However, DSA does not mandate default neutral settings in all cases, nor does it regulate the choice where users intentionally prioritize better usability over higher transparency. The pre-selected choice (for example, language) and inability to compare information flow on different parameters may reinforce the propaganda effect and create information bubbles. The recipients cannot preselect human content moderators over automated content moderation.

To conclude, transparency by choice in digital services cannot be equalized to the scope of neutrality and impartiality of a civil service in an open government. Given the criticism over content moderation and the unprevented impact of the spread of misinformation, hate, propaganda, and fake news, transparency by choice is not future-proof as expected.

4. Conclusions

1. The meaningful transparency framework implemented in the EU digital acquis is experimental and lacks conceptualization.

[78] *From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation*, cit., 38.

Analysis of transparency measures suggests that the target audience, objectives, and scope of application differ and are context-dependent. Therefore, transparency measures are not standardized enough to serve as universal standards.

2. Meaningful transparency standards in the Digital Services Act comprise elements from two legal regimes. They are constructed from modified governmental transparency measures (transparency by rules, procedural balance tests are borrowed) and new transparency measures that are specific to digital services. The synergy of distinct transparency measures is based on functional necessity for transparency and impact to human rights and freedoms.

3. Newly introduced transparency measures, such as transparency by numbers, data and design, are result – and not process – oriented. The depth of practical application of these measures yet needs to be tested in practice. Practical and legal significance of these measures, inter alia, depend on the interaction of multiple stakeholders and their legal obligations.

4. Content moderation transparency measures, risk assessment tests are drafted to address the systemic challenges to human rights and freedoms post factum. The impact to human rights protection would be improved if transparency of content moderation and systemic risks in providers' activity includes ex-ante transparency measures.

Fundamental Values of Data Protection Law: Autonomy vs the Megamachine

Petro Sukhorolskyi*

Abstract: The chapter is dedicated to the study of values most often associated with the right to the protection of personal data. It is argued that nowadays the impact of data processing technologies on human rights and democratic order has already gone far beyond invasion of privacy; therefore, focusing only on this value and this right does not allow to capture the complex reality and comprehend the threats. Thus, it is proposed to analyse problems with personal data taking into account a new totalitarian threat which is fuelled by current digital trends. With this in mind, an attempt is made to demonstrate the fundamental role of personal autonomy and to prove that it should be the basis for justification for the restrictions imposed on large companies and governments. It is concluded that the assertion of individual's autonomy should be done both at the constitutional level and through the shaping of social norms as well as restructuring the architecture of cyberspace on the principles of democracy, transparency, and decentralisation.

Keywords: personal data; values; autonomy; right to privacy; digital totalitarianism; surveillance; artificial intelligence; big data

With this new 'megatechnics' the dominant minority will create a uniform, all-enveloping, super-planetary structure, designed for automatic operation. Instead of functioning actively as an autonomous personality, man will become a passive, purposeless, machine-conditioned animal…
Lewis Mumford, 1967[1]

* *Associate Professor, Lviv Polytechnic National University, Lviv, Ukraine. Email: sukhorolsky@gmail.com*

[1] L. Mumford, *The Myth of the Machine: Technics and Human Development*, Harcourt, New York, 1967, p. 3.

1. Introduction

Over the past decades, more and more challenges and problems related to personal data (hereinafter – PD) have arisen. Data protection law is becoming increasingly complex. However, legal reforms in this area are carried out mostly by supplementing the existing norms, and not by revising the foundation laid half a century ago when the technological, economic, and social realities in the world were completely different. At the same time, in expert circles, the opinion that something needs to be changed radically is becoming more and more widespread, since many legal prescriptions are becoming more difficult to implement. New developments in the field of big data and artificial intelligence (hereinafter – AI) clearly do not fit into the traditional ideas regarding the rules of PD processing, and there is no general consensus on how to regulate them. In addition, there are doubts whether any regulation will be effective in these cases. The situation is further complicated by significant differences between approaches in various countries, even in those that are historically and culturally similar.

Thus, data protection law is at a crossroads, and it is not clear in what direction it is going to change in the future. One of the main reasons for the existing problems is the significant differences in attitudes towards the regulation of data processing in society and the need for restrictions and interventions. Meanwhile, the conflict of interests between various actors in this area is becoming more obvious and acute, but it is difficult to identify the root of the problem behind manipulations and lobbying campaigns. An analysis of the right to data protection through the prism of the values underlying it will help clarify this. In this chapter, we will try to find out the meaning of a number of values most often associated with the protection of PD, as well as to prove that adequate regulation of data processing is of fundamental importance for society and the international community.

2. The weight of the past

When at the dawn of computerization, the need for the development of special rules regarding PD arose, already existing legal principles and approaches, primarily those related to privacy protection, provided the basis for them. At that time, very few legal scholars suspected how fundamental the upcoming transformations would be, and a number of experts in other fields, although they often sensed the powerful wind of change, could not fully understand exactly where it was blowing. The prospect of the availability of massive amounts of information in publicly available computer networks was regarded only as a great boon, and robots were depicted as separate beings with individual human traits.[2] Based on past experience, it seemed that the main concern was unjustifiable isolated invasions of privacy and the main challenge was to ensure the free and secure flow of data across borders to stimulate economic development.

Accordingly, the guidelines developed by the Organisation for Economic Co-operation and Development in the 1970s were entitled: "On the Protection of Privacy and Transborder Flows of Personal Data".[3] The same reference points, perhaps somewhat smoothed, remained intact in later legal acts and documents. For example, the Convention 108 of the Council of Europe in its preamble actually establishes two main goals that must be reconciled and balanced, namely: ensuring the right to the respect for privacy as well as guaranteeing the free flow of information between peoples.[4] Directive 95/46/EC defined its main purpose as protecting "the fundamental rights and freedoms of natural

[2] Such are the robots in the classic science fiction stories by Isaac Asimov (A. Asimov, *I, Robot*, Gnome Press, New York, 1950).

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, 2002, https://doi.org/10.1787/9789264196391-en

[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 28.01.1981.

persons, and in particular their right to privacy with respect to the processing of personal data".[5]

Later, however, it became clear to European legislators that privacy is definitely not enough to balance all interests and that the processing of PD affects much more human rights. In this way, a consensus was formed regarding the recognition of a new human right – the right to the protection of personal data. It was enshrined in the Charter of Fundamental Rights of the European Union, the updated Convention 108+ of the Council of Europe, and the EU's General Data Protection Regulation which replaced Directive 95/46/EC. Nevertheless, where this right comes from and what fundamental values it protects – the answer to these questions remained vague and ambiguous. The GDPR provides that the right to the protection of personal data "is not an absolute right" and "must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".[6] But the mentioned function and balancing directly depend on what values the specified right protects. The centrality of privacy among these values has given rise to objections and misunderstandings in other countries, primarily in the US, as to whether the significant restrictions and obligations on businesses contained in the GDPR are really justified in a free and open democratic society.

As a result, a somewhat paradoxical situation arose: despite the high level of globalization in this area, regulatory approaches in various countries still differ significantly, and the situation is unlikely to change in the near future. Madeline Carr and Jose Tomas

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 1.

[6] 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), Rec. 4.

Llanos explore the differences in these approaches, including their rationales, particularly in the US, the EU, and China. They point out that the problem can be overcome by "striking a bargain between all actors"[7] and repeatedly refer to the need of supporting innovation and the further development of the data economy as the main goals of future global regulatory framework, though they say little about the values of the other side which require no less attention. In our opinion, this is not only about privacy and not so much about privacy, and the main focus on privacy is more of an obstacle than helping to solve the problem with PD. Changes in the technological environment only confirm this, since in the age of big data and AI, the PD protection framework is becoming less and less suitable and effective.[8]

3. The problem with privacy

Having become a central aspect of the protection of individual's rights in the conditions of increasing data collection by governments and business, the idea of privacy began to expand endlessly and has acquired more and more new dimensions and meanings. As a result, the former negative right to respect for private life in connection with the right to the protection of PD has increasingly become interpreted as implying positive obligations not only for the state, but also for private entities.[9] Some researchers who justify the fundamental importance of privacy even consider it a "constitutive element of a democratic society".[10] However, not everyone agrees with such conclusions and arguments, and this

[7] M. Carr, J. T. Llanos, *Data: Global governance challenges*, in T. G. Weiss, R. Wilkinson (eds.), *Global Governance Futures*, Routledge, London and New York, 2022, p. 296.

[8] A. Mantelero, *Big data and data protection*, in G. G. Fuster, R. V. Brakel, P. de Hert (eds.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, Edward Elgar, Cheltenham, 2022, pp. 335–357.

[9] Guide on Article 8 of the European Convention on Human Rights, European Court of Human Rights, Council of Europe, 31 August 2022, pp. 8–10.

[10] S. Spiros, *Reviewing Privacy in an Information Society*, in *University of Pennsylvania Law Review*, 135, 1987, p. 732.

is the key problem. Therefore, it is important to pay due attention to the arguments of those who deny the fundamental importance of privacy and who, as a rule, are supporters of less binding approaches to the regulation of PD processing. This allows us to understand that their positions are by no means unfounded, and hence privacy is not such a reliable and indisputable value to be the main foundation for data protection law.

First of all, within the sceptical view, privacy is often considered a derivative value that cannot compete equally with the main values of a democratic society, in particular such as freedom, security, or progress.[11] For example, Maarten van Swaay believes that the value of privacy is instrumental, rather than intrinsic, and it cannot be claimed as a separate human right.[12] Judith Jarvis Thomson and Henry John McCloskey consider privacy a derivative right that can always be derived from other values and rights.[13] Some researchers point out that the liberal value of privacy is relatively small, or at least it is much smaller compared to established liberal values, such as freedom of speech, freedom of market transactions, and economic growth.[14] Diane Michelfelder believes that privacy should be considered not as a separate value but as a value cluster within which various individual and social interests are intertwined.[15] However, for its application in practice, such an approach requires complex and ambiguous procedures for establishing and balancing numerous

[11] E. W. Spurgin, *The End of Romance and the Value of Privacy*, in *North American Philosophical Publications*, 20(3), 2006, p. 248.

[12] M. van Swaay, *The Value and Protection of Privacy*, in *Computer Networks and ISDN Systems*, 26(4), 1995, p. 149.

[13] J. J. Thomson, *The Right to Privacy*, in *Philosophy & Public Affairs*, 4(4), 1975, p. 313; H. J. McCloskey, *Privacy and the Right to Privacy*, In *Philosophy*, 55(211), 1980, p. 31.

[14] B. de Bruin, *The liberal value of privacy*, in *Law and Philosophy*, 29, 2010, p. 506.

[15] D. P. Michelfelder, *The moral value of informational privacy in cyberspace*, in *Ethics and Information Technology*, 3, 2001, p. 133.

interests in each specific case and does not allow making general conclusions about key values.

Another important issue concerns the boundaries of privacy. If on the one side there is privacy, the essence of which as a value is questionable, and on the other side – such fundamental interests as freedom of speech, security, and economic growth, then the boundaries of privacy should be narrow enough. Obviously, these boundaries should protect an individual from such obvious violations as home invasion or spying on intimate moments, but the vast majority of PD cases, from this point of view, do not involve such a gross invasion of privacy and should not be subject to strict state regulation. From this arises the belief that the right to privacy is not a fundamental human right, but it is certainly an essential social good that can be bought with money. And we can easily find confirmation of this in the surrounding reality, since in order to get a separate compartment in a train, an individual ward in a hospital, a separate accommodation, or a personal office at work, you need to pay a lot of money or have a relatively high status.[16] At the same time, conditions in shelters or hospitals for the poor, in cheap transport or at hostels are far from ensuring privacy. Most people on earth can only dream of the level of privacy that an individual home or car provides. Similarly, you can also buy a space of greater privacy on the Internet where there will be no intrusive advertising and manipulation, but you have to pay for it. And if one chooses free or cheap analogues, then one's claims to privacy look unfounded. Thus, if privacy is considered a social good rather than a civil right, then this sphere should be regulated by private agreements and without state interventions and restrictions.

The common understanding of privacy presupposes the existence of a specific intrusion that can be recorded, proven,

[16] J. Andre, *Privacy as a value and as a right*, in *The Journal of Value Inquiry*, 20, 1986, p. 312.

and measured. This is one of the prerequisites for balancing the right to privacy with competing rights and interests, but in the current conditions recognizing such a specific intrusion is often extremely difficult. Such a problem is relevant both in the cases of comprehensive state surveillance and in the cases of mass manipulations based on PD by large companies. In this regard, in the Handbook of European data protection law, developed by the Council of Europe and the EU, it is stated that where "masses of personal data or information about individual behaviour are collected, processed and evaluated", measuring "the extent to which privacy and personal data may be affected is not possible".[17] According to Bart van der Sloot, the balancing test is not suitable for privacy-related cases involving big data both because of the difficulty of proving harm and problems with weighing of interests.[18] In view of all this, the issue increasingly shifts to a general and abstract level where it is necessary to take into account not only numerous interests not directly related to a specific case but also existing and potential risks in various areas.[19] This complicates the picture so much that behind the veil of complex procedures it becomes difficult to reveal the main point. And in many cases, it is practically impossible to carry out such a large-scale impact assessment. For example, Taner Kuru and Iñigo de Miguel Beriain note that if we try to balance all the interests related to the processing of personal genetic data, "this could become a

[17] *Handbook of European data protection law*, European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 354.

[18] B. van der Sloot, *How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one*, in *Information & Communications Technology Law*, 24(1), 2015, pp. 98–101.

[19] A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 34, 2018, pp. 754–772; H. Miyashita, *Human-centric data protection laws and policies: A lesson from Japan*, in *Computer Law & Security Review*, 40, 2021, 105487.

nightmare for practitioners",[20] and Yaniv Heled and Liza Vertinsky believe that "the current focus on privacy of genetic information fails to capture the complex reality".[21]

Technological progress gives rise to more and more innovations that literally break privacy-related structures and further confuse the situation. For example, anonymisation can no longer be considered a guarantee of one's privacy,[22] and the implementation of the data minimisation principle may not only not help protect the rights of an individual, but also hinder the detection of violations of these rights, in particular the right to non-discrimination.[23] The concept of sensitive data, which is important for privacy, is gradually losing its meaning, as the boundaries between sensitive and non-sensitive data are becoming blurred, and the former are increasingly easier to deduce from the latter.[24] For many violations and manipulations related to targeting, segregation, and discrimination, it is not at all necessary to store and process PD.[25]

Another interesting example concerns the right to be forgotten which, given its ambiguity, has attracted the attention of many experts and scholars. On the one hand, people who want information about them removed from the Internet intuitively

[20] T. Kuru, I. de Miguel Beriain, *Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR*, in *Computer Law & Security Review*, 47, 2022, p. 6.

[21] Y. Heled, L. Vertinsky, *Genetic paparazzi: Beyond genetic privacy*, in *Ohio State Law Journal*, 82:3, 2021, p. 413.

[22] P. Quinn, *The Anonymisation of research data – A pyric victory for privacy that should not be pushed too hard by the EU data protection framework?* in *European Journal of Health Law*, 24, 2017, pp. 1–21.

[23] M. van Bekkum, F. Z. Borgesius, *Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?* in *Computer Law & Security Review*, 48, 2023, 105770.

[24] P. Quinn, G. Malgieri, *The difficulty of defining sensitive data – The concept of sensitive data in the EU data protection framework*, in *German Law Journal*, 22, 2021, pp. 1583–1612.

[25] M. Galič, R. Gellert, *Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab*, in *Computer Law & Security Review*, 40, 2021, 105486.

believe that they "have a right to it". On the other hand, many such cases clearly go beyond the boundaries of privacy because they concern public acts, professional activities, or violations of law. If an individual asks Google to remove links that lead to a bona fide newspaper article, we understand that this newspaper cannot be accused of privacy invasion. In the case of balancing the right to be forgotten with opposing interests, such as freedom of expression, it is extremely difficult to determine the abstract weight of the former and compare it with the abstract weight of opposing interests, principles, and values.[26] All this leads to very different assessments of the right to be forgotten in the works of European and American researchers.[27]

In view of all these complexities, privacy does not appear to be a reliable and indisputable basis for justifying the numerous restrictions and obligations related to data processing that must be introduced in order to guarantee human rights and democracy. At the same time, while there are endless debates about the role of privacy, technology is rapidly developing, and the socio-political system, as will be shown in the following sections, is confidently moving in the opposite direction.

4. Dignity, liberty, equality, and other values

The situation is similar with a number of other values that are believed to necessitate the protection of PD. In particular, in Europe, dignity is considered a value that underlies not only the right to the protection of PD but also the entire system of human rights. Without diminishing the fundamental importance

[26] We are talking about abstract weight according to the theory of balancing by Robert Alexy (R. Alexy, *On balancing and subsumption. A structural comparison*, in *Ratio Juris*, 16(4), 2003, pp. 433–449).

[27] P. Bernal, *The EU, the US and Right to be Forgotten*, in S. Gutwirth, R. Leenes, P. de Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer, Dordrecht, 2013, pp. 61–77.

of human dignity, it is still worth noting that proving unjustified interference with this right and value is an impossible task in many cases involving PD. Massive collection and processing of personal and other data by large companies or government institutions for economic and security purposes, which concern millions and billions of people, can hardly be qualified as interference with human dignity. In addition, the latter is primarily associated with protection against particularly severe violations of human rights specified in the first chapter of the Charter of Fundamental Rights of the EU, such as torture, slavery, and other inhumane practices.[28]

Another relevant value is liberty. Negative liberty, i.e. freedom from interference from the outside, is clearly the basis of the right to privacy.[29] The right to the protection of PD is undoubtedly related to both negative and positive liberty. However, the dimensions of human freedom are very diverse, and the result of balancing the freedom underlying the right to the protection of PD with, for example, freedom of speech or freedom of economic activity, especially in cases where the interference with the former is not very obvious, will, as a rule, not be in favour of PD protection.[30] Moreover, one cannot ignore the argument that in cyberspace a data subject not only loses some freedom due to the activities of large companies or governments but also gains new freedom related to the digital products of the same companies or governments. Thus, the individual's interest in protecting his or her data is opposed not only by the interests of the opposite parties but also by his/her own interest in using the full benefits of informatisation expressed in specific services and platforms on the Internet. That is why, the leaders of Silicon Valley claim that the user's consent to the

[28] *Charter of Fundamental Rights of the European Union*, Official Journal of the European Communities, 18.12.2000, C364/1, art. 1–5.

[29] I. Berlin, *Two concepts of liberty*, in I. Berlin, *Four Essays On Liberty*, Oxford University Press, 1969, p. 118–172.

[30] J. Andre, *Privacy as a value and as a right*, cit., pp. 314–315.

conditions offered by the platform and which provide for the large-scale collection and use of PD is something like a new social contract according to which users "voluntarily relinquish things they value in the physical world – privacy, security, personal data – in order to gain the benefits that come with being connected to the virtual world".[31] So, the situation with freedom as an underlying value for the right to the protection of PD is also confusing and ambiguous.

Another value that has become very relevant recently due to the improvement of data processing algorithms is equality in the sense of non-discrimination. It suddenly turned out that an Internet user can become an object of discrimination even when his/her PD is not stored and processed simply because algorithms, trained on PD of many other people, are able to make a discriminatory decision based on open data in almost real time.[32] This somewhat pushed the privacy debate aside and led to a reorientation of focus to the creation of more comprehensive impact and risk assessment systems.[33] However, the emphasis on non-discrimination has its drawbacks. Firstly, the problem of discrimination is quite narrow and does not cover all contradictions and conflicts of interests in this area. Secondly, the awareness of this problem leads to the search for technological and point solutions rather than to the identification and elimination of its root causes. Thirdly, there are doubts whether it is even possible to eliminate such discrimination in current realities where, as Anastasiya Kiseleva and Paul Quinn point out, "algorithmic bias creeps into AI systems in a myriad of ways and can exist in many shapes and forms".[34]

[31] E. Schmidt, J. Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*, Knopf Doubleday Publishing Group, New York, 2013, p. 263.

[32] M. Rhoen, Q. Y. Feng, *Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science*, in *International Data Privacy Law*, 8(2), 2018, pp. 140–159.

[33] A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, cit., pp. 754–772.

[34] A. Kiseleva, P. Quinn, *Are You AI'S Favourite? EU Legal Implications of Biased AI Systems in Clinical Genetics and Genomics*, in *European Pharmaceutical Law Review*, 5(4), 2021, p. 158.

Thus, it can be concluded that all the mentioned values, despite their importance for the regulation of data processing, cannot serve as the main foundation for the development of solutions related to contemporary challenges. These challenges and threats are the outcome of a significant imbalance of power in cyberspace and, in general, in society in favour of entities that have vast amounts of data and technological power at their disposal, and we will examine these issues in detail in the next section.

5. The threat of totalitarianism

Over the past decades, there has been a constant increase in the amount of data that requires enormous computing power to process. This is one of the factors that determine the tendency towards centralisation, while the authors of early concepts and images of the information society, on the contrary, considered decentralisation to be a key characteristic of the future social system.[35] During this time, we have witnessed the emergence of huge private companies that are almost global monopolies in their fields. Meanwhile, the state's ability to control information flows has not disappeared and in many cases has even significantly strengthened. If until recently the main problem was considered to be the malicious use of available PD by the authorities and business, now attention is focused on the potential of key actors to directly influence people's behaviour and shape their environment through information manipulations. All this makes us seriously address the threat of totalitarian control which has become much closer than in pre-computer times.

The rise of digital totalitarianism is discussed in many works. In particular, Cathy O'Neil in the book "Weapons of Math Destruction"

[35] A. Toffler, *The Third Wave*, William Morrow and Company, New York, 1980, p. 84, 187; J. Naisbitt, *Megatrends: Ten New Directions Transforming Our Lives*, Warner Books, New York, 1984, pp. 103–141.

shows how the formation of increasingly monolithic power in society is combined with its rapid implementation of the latest technologies of mass manipulation.[36] Shoshana Zuboff in the work "The Age of Surveillance Capitalism" characterizes the modern heir of totalitarian power, an instrumental power, which tries to achieve complete automation and control of society through means of behaviour modification as well as unprecedented asymmetry of knowledge.[37] Evgeny Morozov in the book "The Net Delusion" convincingly demonstrates how modern information technology destroys the foundations of democracy.[38] Dennis Morgan believes that "smiley-faced" inverted totalitarianism, which combines features of dystopias by George Orwell and Aldous Huxley, is strengthening in the modern surveillance society.[39]

In order to illustrate exactly how this happens, we use the "pathetic dot theory" by Lawrence Lessig presented in his book "Code and Other Laws of Cyberspace".[40] According to Lessig, society is regulated by four main forces: social norms, the market, architecture, and the law. And it is not difficult to trace how all of them push us towards centralisation and total supervision. In particular, social norms under the influence of large companies increasingly encourage the sharing of private information and lead to the spread of a "don't care" attitude when it comes to general surveillance. Diane Michelfelder writes in her 2001 article: "Some e-commerce providers have begun to directly monitor visitors

[36] C. O'Neil, *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown, New York, 2016.

[37] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019.

[38] E. Morozov, *The net delusion: How not to liberate the world*, Public Affairs, New York, 2011.

[39] D. R. Morgan, *Inverted totalitarianism in (post) postnormal accelerated dystopia: the arrival of Brave New World and 1984 in the twenty-first century*, in *Foresight*, 20(3), 2018, pp. 221–236.

[40] L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

to their Web sites in an attempt to market their products more effectively. … For some, this 'customer service' appears as an extremely intrusive invasion of privacy".[41] Just two decades later in 2024, interventions of this kind have become routine and are applied by almost all online platforms, and any dissatisfaction with this state of affairs seems marginal and hardly affect anything. As a result of the ability of dominant actors to shape social norms that benefit them, these norms change rapidly and cease to fulfill their former role in society, since, as Lewis Mumford points out, "containers can serve their function only if they change more slowly than their contents".[42]

The second regulator is the market, about which the head of the Uber company said the following: "We are not setting the price. The market is setting the price. … We have algorithms to determine what that market is."[43] Ramsi Woodcock believes that with the advent of big data comes the end of the free market, and it means that a new "regulatory Phoenix" will rise from the ashes of the market, "potentially more effective and just than ever before".[44] However, what is overlooked is the fact that the market is decentralised, and such a new regulator is terrifying in its scale and centralisation. The third regulator, architecture, in our case appears in the form of software and hardware underlying cyberspace. Few today doubt that technology has long been designed to increase data collection, surveillance, and manipulation. Still, Lessig is convinced that if desired, this architecture could have

[41] D. P. Michelfelder, *The moral value of informational privacy in cyberspace*, cit., pp. 134–135.

[42] L. Mumford, *The Myth of the Machine: Technics and Human Development*, cit., p. 88.

[43] M. Wohlsen, *Uber boss says surging prices rescue people from the snow*, in *Wired*, 17.12.2013, URL: https://www.wired.com/2013/12/uber-surge-pricing/

[44] R. Woodcock, *Big data, price discrimination, and antitrust*, in *Hastings Law Journal*, 68, 2017, p. 1416.

been created in a completely different way.[45] By not reacting in time, society allowed the dominant actors, i.e. corporations and powerful governments, to implement a system that corresponds exclusively to their interests and their vision. The last regulator, law, at least in some jurisdictions, tries to do something against the system of total supervision and control, but shifting the focus of legislators' attention to side issues and overlooking the main problem does not allow it to be done effectively.

The reality toward which our civilisation is moving was detailed more than half a century ago in Lewis Mumford's seminal two-volume work "The Myth of the Machine".[46] In it, he treats the entire history of mankind as the confrontation of decentralised forms of social organisation and efforts to construct the Megamachine, the elements of which are human individuals. Mumford foresees that the computer "will be able to find, to locate, and to address instantly, by voice and image, … any individual on the planet: exercising control over every detail of the subject's daily life".[47] The finale triumph of all this "would be the consolidation of every human activity into an autocratic and monolithic system", that "would produce a mode of existence in which functions that cannot be canalized into the system would be suppressed or extirpated".[48]

The outstanding dystopias of the 20th century by Yevgeny Zamyatin, Aldous Huxley, and George Orwell, which have become relevant and popular again today, help us better understand the essence and key characteristics of the new totalitarianism. In them, we see that privacy has been completely destroyed. For example,

[45] L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, Basic Books, New York, 2006, pp. 306–310.

[46] L. Mumford, *The Myth of the Machine: Technics and Human Development*, cit.; L. Mumford, *The Myth of the Machine: The Pentagon of Power*, Harcourt, New York, 1970.

[47] L. Mumford, *The Myth of the Machine: The Pentagon of Power*, cit., p. 274.

[48] Ibid., p. 330.

in Huxley's novel, the main female character thinks that in private one can only have sex and nothing else[49] (such are the new social norms shaped by the system), and in Zamyatin's book, people can lower the shades in their transparent houses also only for this purpose.[50] However, if we consider the essence of the problem, it is not difficult to understand that the private life of individuals in itself is of little interest to the totalitarian system. Its main goal is to destroy any manifestations of individuals' *autonomy* and to turn them into obedient automatons – cogs in a big machine. Therefore, it is the autonomy that is the main value and the main principle on which data protection law should be based in order to restore lost balances. Mumford was well aware of this problem, warning that comprehensive digital surveillance is "not just the invasion of privacy, but the total destruction of autonomy: indeed the dissolution of the human soul".[51]

6. The fundamental importance of autonomy

Autonomy is mentioned in most of the works dealing with the values underlying the protection of PD, but it is usually considered in the context of the right to privacy and as a means of justifying it. This does not allow to see the bigger picture. A common argument is that privacy in cyberspace supports the growth of individual autonomy, and therefore it strengthens democratic authority.[52] It is difficult to disagree with this, but it does not cover such important cases where autonomy itself, and not privacy, is at risk due to unfair data processing. Andre claims that "the connection between privacy and autonomy is considerably less than is

[49] A. Huxley, *Brave New World*, Harper Perennial, New York, 2006, p. 88.

[50] Y. Zamyatin, *We*, Avon Books, New York, 1987, p. 18.

[51] L. Mumford, *The Myth of the Machine: The Pentagon of Power*, cit., p. 274–275.

[52] D. P. Michelfelder, *The moral value of informational privacy in cyberspace*, cit., p. 133.

generally assumed".[53] This may indeed be true, since autonomy is closer to freedom than to privacy. However, when it comes to PD protection, such an argument is frequently used to prove that legal restrictions on the activities of large Internet companies are unjustified. We cannot agree with this position.

Undoubtedly, privacy is a very important issue, but it is only part of the current problem and probably not the main one. Many problems regarding data processing should be viewed through the prism of a direct conflict of autonomy with other important values (security, economic freedom, progress, etc.). Furthermore, it must be recognized that the very terminology used in this field (data privacy, personal data protection) is not perfect, because it focuses our attention primarily on privacy and data related to a specific person, while technological realities have already gone much further.[54] Therefore, the main goal should be considered not so much the protection of the individual or the protection of his/her data as the establishment of adequate and fair balances in the field of data processing.

Placing autonomy at the center of our attention makes it easy to understand the nature of a variety of complex problems associated with PD. For example, the right to be forgotten should be understood as an attempt by European legislators to protect autonomy, since having the right to erase or not erase information about your past life or, in general, having the right to start life with a clean slate is exactly what allows an individual to be an independent agent. While talking about privacy, Andre notes that a "door which one can open and close is better than a wall".[55] This is a good metaphor to illustrate the difference between

[53] J. Andre, *Privacy as a value and as a right*, cit., p. 312.

[54] M. Galič, R. Gellert, *Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab*, cit.; A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, cit., pp. 754–772.

[55] J. Andre, *Privacy as a value and as a right*, cit., p. 313.

privacy and autonomy: the former is like a wall behind which no one except very close people should penetrate, while autonomy is more related to a door through which one can invite even the whole world inside, but when the need arises get them out of the house.

In his article, James Rachels discusses the fact of different human behaviour in different relationships which leads to speculation about the "real" person and the various "masks" that the person wears.[56] This gives rise to the argument that if a person is authentic and does not put on a mask, then there is no need for privacy. If we take autonomy as a basis of reasoning, then it becomes obvious that it is precisely the sphere of manifestation of individual's autonomy and no one, except a personal psychologist, has the right to interfere in such things. One of the early publications on the impact of big data on society by Neil Richards and Jonathan King describes three main problems that this technology creates, namely transparency, identity, and the balance of power. The authors conclude that such issues should be settled taking into account "values we have long cherished like privacy, identity, and individual power".[57] However, the main value that encompasses the three political issues is exactly autonomy. It is it, and not privacy, that is the main bulwark against various types of manipulation.

If we consider the practical side of the problem, it is clear that there is no separate right to autonomy in international law, even in the narrow sense as it is in the case of the right to dignity, although the idea of its introduction is not new.[58] Autonomy is the foundation of all human rights of the first generation,

[56] J. Rachels, *Why privacy is important*, in *Philosophy & Public Affairs*, 4(4), 1975, p. 326.

[57] N. M. Richards, J. H. King, *Three Paradoxes of Big Data*, in *Stanford Law Review Online*, 66:41, 2013.

[58] K. Möller, *The Global Model of Constitutional Rights*, Oxford University Press, 2012, pp. 73–95.

because without it they lose their meaning; it is also an important prerequisite for a social contract, since such a contract can be concluded only by independent and autonomous individuals. Over the past centuries, many works have been written about the importance of autonomy in this context.[59] Therefore, it is a strong basis for argumentation aimed at justifying the limitations of the influence of dominant actors in cyberspace and the construction of a decentralised online architecture. Meanwhile, this issue cannot be resolved at the individual level by weighing interests or risks in each specific case, since we are talking about fundamental things and general political principles that have to be established at the constitutional level.

Obviously, there can be no question of a "new social contract" through the voluntary relinquishment of privacy, which is talked about in Silicon Valley,[60] for it is not only and not so much about privacy. Also, the weighing of interests by executive and judicial bodies is not very suitable here. The European Court on Human Rights faced this problem in the case of Roman Zakharov v. Russia regarding state surveillance. In its decision, the Court points out that it is not its task "to review the relevant law and practice in abstracto", but still it is forced to depart from this rule in order to protect the rights of the individual.[61] In this context, van der Sloot notes that the balancing test is not what is needed in big data cases, because the matter is not about the violation of

[59] S. Buss, A. Westlund, *Personal Autonomy*, in E. N. Zalta (ed.) *The Stanford Encyclopedia of Philosophy*, Spring 2018, URL: https://plato.stanford.edu/archives/spr2018/entries/personal-autonomy/; F. Neuhouser, *Jean-Jacques Rousseau and the Origins of Autonomy*, in *An Interdisciplinary Journal of Philosophy*, 54(5), 2011, pp. 478–493.

[60] E. Schmidt, J. Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*, cit., p. 263.

[61] Judgment of the European Court on Human Rights (Grand Chamber) of 4 December 2015, Roman Zakharov v. Russia, ECLI:CE:ECHR:2015:1204JUD004714306, § 164–165.

specific rights, but about evaluating the constitutionality of laws and policies. This is done by constitutional courts based on tests of legality and legitimacy.[62]

As Lessig points out, this balance and these constitutional provisions will by no means appear by themselves: "Constitutions in this sense are built, they are not found. Foundations get laid, they don't magically appear."[63] Such provisions emerge from values, as well as the way they are reconciled. Yet this is not the whole problem, as in our case we are talking about relations that almost always cross state borders, and therefore regulation at the national level is clearly not enough. In the era of globalisation, we have a dense network of international relations at various levels, but we have neither an international constitution nor any kind of global democracy. There is a system of international protection of human rights, but it is aimed at protecting individuals, not at ensuring a global social contract. This allows the powerful to push their interests and replace the social contract with a kind of surrogate. In this way, the dominant actors can avoid responsibility and transfer the risks of their activities in cyberspace to everyone.

The mentioned constitutional provisions should become the starting point for establishing a decentralized cyberspace architecture. As Lessig emphasises, if "code is a lawmaker, then it should embrace the values of a particular kind of lawmaking".[64] For example, studying the issue of algorithmic discrimination, Alvaro Bedoya comes to the conclusion that there is nothing automatic and natural in the implementation of face recognition

[62] B. van der Sloot, *Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities*, in S. Gutwirth, R. Leenes, P. Hert (eds.), *Data Protection on the Move*, Springer, Dordrecht, 2016, p. 434.

[63] L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, cit., p. 4.

[64] Ibid., p. 328.

mechanisms. This is a large-scale and costly activity fueled by specific interests and values.[65] Thus, we must be aware that now "regulation by code" is unfolding in full swing, but this process is completely untransparent and undemocratic.

Under current conditions, Asimov's laws of robotics are increasingly being discussed by legal scholars and practitioners.[66] These laws are a true example of regulation by architecture, as they are integrated into the brains of Asimov's robots.[67] However, his laws govern the behaviour of unrelated individual robots, not a network of robots controlled in real time by a single corporation. Another significant difference is that Asimov describes the threat from machines, and our most pressing problem is the threat from the concentration of power in the hands of a few people and their associations given the worldview they share, namely, the idea that problems must be overcome through the expansion, entrenchment, and strengthening of the megamachine. The resolution of the European Parliament states that humans should have control over intelligent machines at all times.[68] Questions arise – who exactly should control machines and whether uncontrolled AI is really the main threat to us? In this way, the focus is shifted from acute problems of distribution of power in society and international relations to hypothetical problems of the destruction of humanity by machines. Meanwhile, the person and his/her autonomy becomes a secondary issue, and the discussion boils down to the opposition of two unacceptable options: the freedom of innovation for corporations and governments, which is capable of destroying civilization, and the nightmare of a centralized megamachine of total surveillance and control.

[65] A. Bedoya, *Algorithmic discrimination vs. privacy law*, in E. Selinger, J. Polonetsky, O. Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, 2018, p. 236.

[66] Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2018/C 252/25.

[67] A. Asimov, *I, Robot*, cit.

[68] Civil Law Rules on Robotics, European Parliament resolution, cit., para. 3.

7. Conclusions

Data protection law and related fields are currently facing significant challenges and should be reformed taking into account actual threats. With this in mind, research into the values underlying such legal norms is a priority. Since information and data relate to all possible areas of human activity, a number of fundamental values must be taken into account. However, current technological and political trends point to the greatest threat to individual's autonomy, and it is to protect this value that the main attention should be paid.

At the time of its emergence, data protection law was closely related to privacy, but now it is obvious that such a focus is not appropriate and can be misleading. Continuation of business-as-usual approach to policy and lawmaking while ignoring obvious problems can lead to nothing good, since the world is changing fundamentally and irreversibly, and the scale and speed of these changes have no analogues in history. The main problem is that in cyberspace, which has very quickly become an integral part of our reality, there are no such insurmountable limitations as there are in physical space. Therefore, the dominant actors are practically not constrained by anything in the construction of the architecture of cyberspace – indeed, whatever one imagines can be built there. But the lack of proper attention and public discussion on these issues leads to uncontrolled transformations towards the centralisation of power, manipulation of people, as well as the destruction of their personal autonomy. To reduce social resistance, these changes are justified by the interests of safety, efficiency, and progress. It is worth noting that in the Third Reich there was also much that was effective and innovative, but this does not mean at all that it should be repeated.

In the face of the threat of digital totalitarianism, whether with a smiling or a terrible face, people need to remember the main

values that have driven them for centuries and for the affirmation of which many lives have been laid down. These are the values of humanism, liberty, and autonomy, the dominance of which must be asserted in cyberspace regardless of the technological level at which humanity is at a particular moment. The protection of an individual's autonomy from sophisticated manipulation by much more powerful actors should be carried out in parallel on four levels. At the legal level, new constitutional principles as well as relevant international legal instruments are needed to ensure personal autonomy and power balance, taking into account technological reality. According to these principles, the architecture of cyberspace should be rebuilt to guarantee that the Internet develops in line with the rules of open democratic communities, and not a mall[69] or a concentration camp. At the same time, it is important to establish social norms and strengthen a civil culture that is intolerant of general surveillance, data harvesting, large-scale manipulation, opacity, monopoly, and other manifestations of digital totalitarianism. Special attention should be given to counteracting high-tech market manipulation or, even worse, the emergence of a new centralised regulatory "digital Phoenix" instead of the market.

In the near future, with the improvement of technology and the exacerbation of global problems, the temptation will probably increase among people to surrender their autonomy to the megamachine in exchange for stability and a safe and predictable life. Much the same is pushed by modern ideologies popular among the technological elite which focus on threats to existence and see the only way out in the "acceleration of progress" and the final triumph of the megamachine at the stage of the technological singularity. On the other hand, there are serious doubts as to

[69] L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*, cit., p. 287.

whether the problems caused by centralisation can be overcome with the help of an even greater level of centralisation. Perhaps a much more appropriate solution is not to weaken people by turning them into manipulated animals but on the contrary to strengthen their capacity through the affirmation of human autonomy as a basic value and principle of a new data processing law.

Right to be forgotten: configurating a balance between privacy and competing interests in the digital era

Bohdan Karnaukh*

Abstract: The chapter explores the right to be forgotten within the broader framework of privacy rights, focusing on seminal cases and legal developments in Europe. The analysis begins with an examination of the landmark judgment of the Court of Justice of the European Union (CJEU) in the case of Google Spain v. AEPD and Mario Costeja González, which established the foundational principles of the right to be forgotten. Subsequently, it describes territorial outreach of the right, as elucidated in the CJEU's ruling in the case of Google LLC v CNIL. The paper then contextualizes the right to be forgotten within the broader right to privacy context, emphasizing its significance in the digital age. A crucial aspect of the discussion involves the balancing exercise required when considering competing values. The chapter outlines considerations relevant to this balancing exercise, including factors mentioned in the Guidelines on Implementation of the Google Spain case and in Regulation (EU) 2016/679. Moreover, it examines how the European Court of Human Rights (ECtHR) has approached this balancing exercise in its jurisprudence. Finally, the paper concludes that while the right to be forgotten is pivotal for individuals to exert control over their online identities, its exercise must be tempered by a careful consideration of competing interests to ensure a nuanced and balanced approach to privacy protection in the digital era.

Keywords: right to privacy; right to be forgotten; right to erasure; freedom of speech; human rights; search engine operator; data subject

1. Introduction

In the ever-expanding landscape of the digital world, the intersection of privacy rights and freedom of expression has

* *PhD (Law), Associate Professor at the Department of Civil Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. E-mail: b.p.karnauh@nlu.edu.ua*

become increasingly complex and contentious. In the digital age, where vast amounts of personal data are generated, collected, and shared online, the right to privacy faces new challenges and complexities. The proliferation of search engines, social media platforms, and online databases has made it increasingly difficult for individuals to control the flow of information about themselves. Personal information, once published on the internet, can remain accessible indefinitely, potentially leading to reputational harm, discrimination, or other adverse consequences for individuals.

The right to be forgotten addresses this challenge by empowering individuals to request the removal or delisting of their personal information from online platforms, particularly search engine results. By exercising this right, individuals can regain some measure of control over their digital identities and mitigate the potential negative impact of outdated, inaccurate, or irrelevant information circulating online.

The right to be forgotten is closely linked to the right to make mistakes, to be given second chance, and to start anew. Human beings are fallible and may engage in actions or behaviors that they later regret. Making mistakes is a natural part of the human experience and individuals should not be permanently defined or stigmatized by their past actions. The right to be forgotten aligns with this principle, particularly if it relates to past mistakes or indiscretions that no longer reflect person's current circumstances or character.

People should have the opportunity to learn from their mistakes, grow, and reintegrate into society without being unduly burdened by past transgressions. In this vein the right to be forgotten promotes rehabilitation and social reintegration by enabling individuals to move on from past errors or missteps by removing or minimizing their public visibility, thereby reducing the risk of ongoing stigma or discrimination.

The ability to begin anew after facing challenges or setbacks in life is vital for everyone. In this sense, as was aptly noted by Spasybo-Fatieieva and Filatova-Bilous, the right to be forgotten resembles confession in Christian culture.[1] No one should be permanently tethered to his or her past and should have the opportunity to forge a different path or identity for him- or herself. The right to be forgotten supports this principle by allowing individuals to exercise control over their online presence and shape their digital identities in a way that reflects their current aspirations, goals, and values, rather than being defined solely by past events or circumstances.

2. Seminal case: Judgement of the CJEU in case of *Google Spain v. AEPD and Mario Costeja González*[2]

The seminal moment in the development of the right to be forgotten occurred with the landmark ruling by the Court of Justice of the European Union (CJEU) in the case of *Google Spain v. AEPD and Mario Costeja González* in 2014.

In this case Mr. Costeja González, a Spanish citizen living in Spain, in 2010 filed a complaint with the Spanish Data Protection Agency (AEPD) against La Vanguardia Ediciones SL, a publisher of a popular newspaper in Catalonia, Google Spain and Google Inc. The issue was that when someone searched for Mr. Costeja González's name on Google, they found links to two newspaper pages from La Vanguardia dated 1998. These pages contained information about a real estate auction related to legal proceedings regarding Mr. Costeja González's social security debts. He asked La Vanguardia to either remove or change these pages so they didn't include his

[1] Спасибо-Фатєєва І. В., Філатова-Білоус Н. Ю. Критичний аналіз права на забуття з погляду економічного аналізу права. *Право на забуття : зб. ст.* / за ред. І. В. Спасибо-Фатєєвої. Харків : ЕКУС, 2021. С. 136.

[2] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C131/12. Judgment of the Court (Grand Chamber), 13 May 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

personal information; he asked Google Spain or Google Inc. to stop showing these links in search results. He argued that since the legal matters were resolved long ago, the articles were no longer relevant. The AEPD rejected the complaint against La Vanguardia, stating that the publication was legally justified as ordered by the Ministry of Labor and Social Affairs. However, the complaint against Google Spain and Google Inc. was upheld.

Google Spain and Google Inc. separately contested that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional consolidated the cases.

The High Court explained that the cases raise the issue of the obligations of search engine operators concerning the protection of personal data of individuals who do not wish certain information, containing their personal data and published on third-party websites, to be indefinitely located, indexed, and accessible to internet users. The resolution of this question hinges on the interpretation of Directive 95/46 within the context of evolving technologies that emerged subsequent to the directive's enactment.

The Audiencia Nacional decided to suspend the proceedings and refer to the CJEU for a preliminary ruling. One of the questions referred to the CJEU was whether data subject is entitled "to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be "forgotten" after a certain time" (para 89).

Based on the rules laid out in Article 6(1)(c) to (e) of Directive 95/46, the CJEU noted that data processing, which was initially lawful and accurate, might not comply with the directive later on. This happens when the data are no longer needed for the reasons

it were collected or used. It's especially true when the data seem unsuitable, irrelevant, or just not important anymore, or if there's too much of it considering how much time has passed.

Eventually the CJEU found that fundamental rights under Articles 7 and 8 of the Charter allow a person to request that certain information no longer be accessible to the public through search engine results. Typically, these rights take precedence over both the financial interests of the search engine operator and the public's interest in accessing the information when searching for the individual's name. However, there could be exceptions when the public's significant interest in accessing the information, due to reasons like the individual's role in public life, justifies retaining of the data.

3. Territorial Outreach of the right to be forgotten: Judgement of the CJEU in case of *Google LLC* v *CNIL (2019)*[3]

In the lawsuit filed by Google against the French data protection authority, the CJEU was tasked with determining the geographical extent of the right to be forgotten. In 2016, Google was fined €100,000 by the French regulator for its refusal to implement the right to be forgotten on a global scale. Additionally, Google was instructed to enforce the right to be forgotten across all Google domain names, including google.com. Google's stance was that the French data protection authority was only empowered to mandate compliance on the French google.fr domain.

The CJEU clarified that the right to be forgotten does not encompass links displayed on every version of a search engine worldwide. Instead, it applies to search engines associated with domain names of EU Member States, including google.fr, google.

[3] *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-507/17. Judgment of the CJEU (Grand Chamber) of 24 September 2019. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507

it, google.de, and google.nl. Search engine operators are also obligated to employ measures that effectively hinder or significantly discourage internet users from accessing delisted content when conducting searches by name from a Member State.

The CJEU judgement reads:

"where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request" (para 73).

This case has to be contrasted with case of *Eva Glawischnig-Piesczek v Facebook Ireland Limited*,[4] which concerned defamatory statements. Ms. Eva Glawischnig-Piesczek, a prominent figure in Austrian politics, was subjected to defamation on Facebook by a user who shared an article along with harmful comments. Despite her request for removal, Facebook Ireland did not take down the offensive content. Consequently, Ms. Glawischnig-Piesczek pursued legal action, resulting in a court order directing Facebook Ireland to cease publishing any further content containing defamatory remarks or images of her. In compliance, Facebook disabled access to the content in Austria.

One of the questions referred to the CJEU was whether the effect of such an injunction can be extended worldwide. The

[4] *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Case C-18/18, Judgment of the CJEU (Third Chamber), 3 October 2019. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=4157409

CJEU found that Directive 2000/31, in particular Article 15(1), 'must be interpreted as meaning that it does not preclude a court of a Member State from: ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law'.

The different conclusions of the CJEU (as to the territorial range of remedying measures) in the two mentioned cases has to be explained by different treatment of defamation, on the one hand, and truthful statements that have lost their relevance with the passage of time, on the other. Untruthful, defamatory statements should be eliminated without a trace on the global level. Yet the right to be forgotten (which relates to accurate though outdated personal information) is treated differently on different continents and therefore European law confines itself to providing remedy within the EU only.

4. Right to Privacy in General

The right to privacy is a fundamental human right that encompasses the individual's ability to lead an independent life and decide on what aspects of his or her life shall be known to public. In a nutshell, privacy means two types of freedom: freedom to decide what to do with one's own life and freedom to decide what public can know about it.

The latter aspect is all about the individuals' ability to control their personal information and determine how it is collected, used, and shared by others. Overall, the right to privacy is related to various aspects of personal autonomy, dignity, and security,[5] allowing individuals to maintain a sphere of personal space and

[5] Размєтаєва Ю. С. Право бути забутим: витоки і перспективи. *Право на забуття : зб. ст.* / за ред. І. В. Спасибо-Фатєєвої. Харків : ЕКУС, 2021. С. 115–131.

freedom from intrusion or interference by others, including the government, corporations, and other individuals.

In *Khadija Ismayilova v. Azerbaijan* the ECtHR frames the concept of privacy in broad brush strokes:

"The Court notes that the concept of "private life" is a broad term not susceptible to exhaustive definition. As indicated in paragraph 106 above, it is a concept which covers the physical and psychological integrity of a person, and can therefore embrace multiple aspects of the person's physical and social identity. Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world (see *Bărbulescu v. Romania* [GC], no. 61496/08, § 70, 5 September 2017, with further references). Private life may even include activities of a professional or business nature (see *Denisov v. Ukraine* [GC], no. 76639/11, §§ 100–01, 25 September 2018). The Court has also held that everyone has the right to live privately, away from unwanted attention (see *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, ECHR 2003IX (extracts), and *Bărbulescu*, cited above, § 70)".[6]

In *Smirnova v. Russia* the ECtHR adds that right to privacy "secures to the individual a sphere within which he or she can freely pursue the development and fulfilment of his personality".[7]

The right to privacy is recognized and protected by numerous international and national laws, constitutions, and treaties around the world. While the specific scope and protections of the right

[6] *Khadija Ismayilova v. Azerbaijan*, nos. 65286/13 and 57270/14, § 139, 10 January 2019. https://hudoc.echr.coe.int/eng?i=001-188993

[7] *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, 24 July 2003. https://hudoc.echr.coe.int/eng?i=001-61262

to privacy may vary depending on the legal jurisdiction, certain common principles underpin its definition and application.

Right to privacy may be seen as an umbrella term embracing several aspects, such as

informational privacy: concerns an individual's right to control the collection, use, and dissemination of their personal information. It includes safeguards against unwarranted surveillance, data mining, and unauthorized access to personal data by government agencies, businesses, or other entities.

decisional privacy: refers to an individual's right to make autonomous choices and decisions without undue interference or coercion. This includes the right to make personal, medical, reproductive, and lifestyle choices free from government or societal intrusion.

bodily privacy: pertains to the protection of an individual's physical integrity, autonomy, and dignity. It encompasses the right to bodily autonomy, such as the right to refuse medical treatment, the right to control one's own body, and protection against invasive bodily searches or procedures without consent.

territorial privacy: relates to an individual's right to privacy within their physical space, such as their home, workplace, or other private locations. It includes protection against unauthorized entry, surveillance, or monitoring within these spaces.

communicational privacy: involves the protection of an individual's communications, including their correspondence, telephone conversations, emails, and other forms of electronic communication, from interception, surveillance, or unauthorized access.

The right to privacy is often seen as essential for the promotion of human dignity, individual autonomy, and the realization of other fundamental rights and freedoms. It serves as a safeguard against abuses of power, discrimination, and infringements on personal liberties by both state and non-state actors.

However, the right to privacy is not absolute and may be subject to limitations or restrictions in certain circumstances, such as for national security, public safety, public health, or the protection of other fundamental rights. Striking a balance between privacy rights and competing interests is often a complex and ongoing challenge for lawmakers, policymakers, and courts.

5. Right to be forgotten as part of the right to privacy[8]

The right to be forgotten is intimately connected to the broader concept of the right to privacy, as it pertains to the control individuals have over their personal information and digital identities.

In *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*[9] the ECtHR noticed:

"It follows from well-established case-law that where there has been compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise (see *Uzun v. Germany*, no. 35623/05, §§ 44–46, ECHR 2010 (extracts); see also *Rotaru v. Romania*, cited above, §§ 43–44; *P. G. and J. H. v. the United Kingdom*, cited above, § 57; *Amann*, cited above, §§ 65–67; and *M. N. and Others v. San Marino*, no. 28005/12, §§ 52–53, 7 July 2015).

The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the

[8] Yet, there are other views on the status of the right to be forgotten. For the overview see: Размєтаєва Ю. С. Право бути забутим: витоки і перспективи. *Право на забуття : зб. ст.* / за ред. І. В. Спасибо-Фатєєвої. Харків : ЕКУС, 2021. С. 115–131.

[9] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13, §§ 136–137, 27 June 2017. https://hudoc.echr.coe.int/eng?i=001-175121

guarantees of this Article (see *S. and Marper*, cited above, § 103). Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged".

Therefore, the right to be forgotten intersects with various aspects of privacy, first and foremost informational privacy, which concerns the protection of personal data from unauthorized access or use, and decisional privacy, which involves individuals' ability to make choices about their personal information. By allowing individuals to manage the information available about them online, the right to be forgotten helps safeguard their reputation, identity, and informational self-determination.

However, the right to be forgotten also raises complex ethical, legal, and practical considerations, particularly concerning the balance between privacy rights and competing interests such as freedom of expression and public interest in access to information. Critics argue that the right to be forgotten may undermine principles of free speech and transparency by allowing individuals to suppress information that is in the public interest or relevant to ongoing discourse. Moreover, challenges related to the effectiveness of delisting mechanisms, the global nature of online information, and the enforcement of removal requests across different jurisdictions further complicate the implementation of the right to be forgotten.

Therefore, while the right to be forgotten serves to protect individuals' privacy and autonomy, its implementation requires careful consideration of the complex and often competing interests at stake, highlighting the ongoing evolution and adaptation of privacy rights in the digital age.

Like many other human rights, the right to be forgotten is not absolute, and when it clashes with other values and rights (freedom

of expression and right to access to information), meticulous balancing of numerous considerations has to be performed before one can decide whether the right to be forgotten stands or gives way to competing value. The need for this balancing was outlined in the seminal judgment of the CJEU in *Google Spain* case.

6. Balancing exercise: general outline of competing values

Balancing the right to be forgotten against other interests is a complex task that involves weighing privacy rights against competing considerations such as freedom of expression, public interest in access to information, and the responsibilities of digital platforms. This delicate balance is crucial in navigating the multifaceted landscape of the digital age, where individual rights intersect with broader societal needs and values.

One of the primary concerns in balancing the right to be forgotten is its potential impact on **freedom of expression**. Critics argue that allowing individuals to request the removal of information from search engine results may lead to censorship and undermine free exchange of information.[10] It is essential to ensure that the right to be forgotten does not unjustly suppress legitimate expression or restrict public discourse on matters of importance.

Similarly, the right to be forgotten must be balanced against the **public's right to access information**. Information plays a crucial role in fostering transparency, accountability, and informed decision-making in society. Limiting access to information, particularly on matters of public concern, may hinder the public's ability to engage in democratic processes and hold institutions accountable.

[10] Ausloos J. The 'Right to Be Forgotten' – Worth Remembering? (December 9, 2011). Computer Law & Security Review. 2012. Vol. 28. Issue 2. P. 143–152; Rosen J. The Right to Be Forgotten. Stanford Law Review. 2012. Vol. 64. P. 88. https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf

Consideration of the public interest is vital in determining whether certain information should be subject to removal requests. There may be instances where the public interest in accessing information outweighs an individual's privacy rights. Information that is relevant to public health, safety, or the conduct of public figures may be considered to serve the public interest and thus exempt from removal requests.

Digital platforms play a central role in implementing the right to be forgotten, as they are responsible for processing removal requests and delisting information from search results. Platforms must balance the rights of individuals with their obligations to provide access to information and promote free expression. This entails establishing transparent and accountable processes for handling removal requests, as well as ensuring that decisions are made in accordance with relevant legal frameworks and principles.

Another consideration in balancing the right to be forgotten is its potential impact on **innovation and economic development**. Striking the right balance between privacy rights and the interests of businesses and innovation is essential to fostering a thriving digital economy. Excessive restrictions on the processing of personal data or the dissemination of information may stifle innovation and hinder economic growth.

Given the borderless nature of the internet, achieving **consistency and harmonization** in the application of the right to be forgotten across jurisdictions is crucial. Divergent legal standards and regulatory approaches may lead to confusion and conflicts, undermining the effectiveness of the right to be forgotten and complicating compliance for digital platforms operating in multiple jurisdictions.

In navigating these various interests, policymakers, regulators, and digital platforms must engage in a nuanced and transparent decision-making process. This process should involve careful

consideration of the specific circumstances of each case, taking into account the rights and interests of all stakeholders involved. Clear and predictable legal frameworks, coupled with robust mechanisms for oversight and accountability, are essential for achieving a balanced approach to the right to be forgotten that upholds privacy rights while preserving the values of free expression, access to information, and public interest.

7. Considerations relevant to balancing exercise in Guidelines on Implementation of *Google Spain* case

On 26 November 2014 Data Protection Working Party adopted Guidelines on the Implementation of the Court of Justice of the European Union Judgment on *Google Spain* case[11]. The core issue addressed in the Guidelines is balance striking. The Working Group notes:

"In relation to the balance of interests that may legitimate the processing carried out by the search engine, according to the ruling, the rights of the data subject prevail, as a general rule, over the economic interest of the search engine, in light of the of the potential seriousness of the impact of this processing on the fundamental rights to privacy and data protection. These rights also generally prevail over the rights of internet users to have access to the personal information through the search engine in a search on the basis of the data subject's name. However, a balance has to be struck between the different rights and interests and the outcome may depend on the nature and sensitivity of the processed data and on the interest of the public to have access to that particular information on the other, an interest which may vary, in particular, by the role played by the data subject in public life (§ 81)".

[11] Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12. https://ec.europa.eu/newsroom/article29/items/667236/en

To provide European data protection authorities with a toolbox to conduct balancing exercise Working Group developed a set of questions, each question indicating a separate criterion that must be weighed while deciding whether the applicant should be granted the removal of his personal data. The set includes the following questions:

"1. Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?

2. Does the data subject play a role in public life? Is the data subject a public figure?[12]

3. Is the data subject a minor?

4. Is the data accurate?

5. Is the data relevant and not excessive?

a. Does the data relate to the working life of the data subject?

b. Does the search result link to information which allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant?

c. Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?

6. Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?[13]

7. Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?

[12] For the the definition of a 'public figure' see the the Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy: 'Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain'. Yet the Working Group emphasizes that person who 'plays a role in public life' is even broader than 'public figure'.

[13] According to Art 8 of the Directive 95/46/EC data is considered sensitive when itreveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

8. Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?

9. Does the search result link to information that puts the data subject at risk?

10. In what context was the information published?

a. Was the content voluntarily made public by the data subject?

b. Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?

11. Was the original content published in the context of journalistic purposes?

12. Does the publisher of the data have a legal power – or a legal obligation – to make the personal data publicly available?

13. Does the data relate to a criminal offence?"

8. Competing interest in Regulation (EU) 2016/679

The right to be forgotten was enshrined in the Regulation (EU) 2016/679[14]. It appears in Art 17 as a part of a broader concept – "right to erasure". The right to erasure encompasses all legal grounds that entitle the data subject to request the erasure of his or her personal data (e.g. withdrawal of consent previously given, unlawful processing of the data etc). The right to be forgotten appears to be one prominent instance where the data subject is acknowledged to have the right to erasure. In particular under Art 17 (1)(a) & (c) the data subject shall have the right to obtain from the controller the erasure of personal data if

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or

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

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).

According to Art 21(1) the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e)[15] or (f)[16] of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

At the same time in Art 17(3) it is recognized that the right to erasure (and the right to be forgotten as a part of it) is not absolute. For this reason, the article contains a list of considerations that may outweigh the person's right to be forgotten. Thus, the right may not apply if data processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

[15] 'Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

[16] 'Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

9. Balancing exercise in the jurisprudence of the ECtHR

Valuable insights on how to operate balancing exercise can be found in the case law of the ECtHR. The Court has deliberated upon the concept of the "right to be forgotten", in the following contexts:[17]

– where media entities maintain archival materials on their online platforms, encompassing personal identifiers such as names and images;[18]

– where individuals accused or suspected of crimes seek the removal of their personal data, including DNA profiles, identity photos, and fingerprints, from databases used for crime prevention and investigation;[19]

– where individuals were unable to obtain the removal of their previous convictions from police records after a specific period of time;[20] and

[17] Guide to the Case-Law of the of the European Court of Human Rights. Data Protection. Updated on 31 August 2022. P. 64. https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG

[18] See: *M. L. and W. W. v. Germany*, nos. 60798/10 and 65599/10, 28 June 2018. https://hudoc.echr.coe.int/fre?i=001-183947

[19] See: *Gaughran v The United Kingdom*, no. 45245/15, 13 February 2020. https://hudoc.echr.coe.int/fre?i=001-200817; *Catt v. The United Kingdom*, no. 43514/15, 24 January 2019. https://hudoc.echr.coe.int/eng?i=001-189424; *Aycaguer v. France*, no. 8806/12, 22 June 2017. https://hudoc.echr.coe.int/eng?i=001-174441

[20] See: *M. M. v. The United Kingdom*, no. 24029/07, 13 November 2012. https://hudoc.echr.coe.int/fre?i=001-114517

– where personal data was kept in security service archives after turning irrelevant, raising questions regarding the necessity of its retention.[21]

Two prominent cases exemplify how the ECtHR strikes a balance between competing interests in the context of the right to be forgotten – *M. L. and W. W. v. Germany* and *Mediengruppe Österreich GmbH v. Austria*.

9.1. Case of M. L. and W. W. v. Germany[22]

In 1993, the applicants were convicted for the murder of a prominent actor and were sentenced to life imprisonment. As their release date approached in 2007, they initiated legal proceedings against various media organizations, seeking the anonymization of archived documents available on their websites from the time of the trial, including an article, a file, and an audio report transcription.

Between 2009 and 2010, despite recognizing the applicants' significant interest in avoiding ongoing exposure to their conviction, the Federal Court of Justice ruled in favor of the media organizations. The court reasoned that:

– The crime and trial had garnered substantial media attention, and the public had a right to access information, including historical research. Media participation in shaping democratic opinion by maintaining accessible archives was deemed integral.

– The applicants attempted to reopen their case proceedings and had actively sought press coverage for their retrial application shortly before their impending release. Furthermore, until 2006,

[21] See: *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, 6 June 2006. https://hudoc.echr.coe.int/eng?i=001-75591

[22] *M. L. and W. W. v. Germany*, nos. 60798/10 and 65599/10, 28 June 2018. https://hudoc.echr.coe.int/fre?i=001-183947

the criminal-defense lawyer's website for the second applicant featured multiple reports about the client.

– The archived documents were clearly labeled to indicate they were not new reports.

– There was a necessity to consider the risk that media outlets, lacking sufficient resources to assess requests for anonymization, might opt to omit identifiable elements from reports, which could later become illegal.

The applicants alleged that refusal of German authorities to oblige media to anonymize online archive material constituted violation of Art 8 of the ECHR (Respect for private life).

The ECtHR reiterated that "where there has been compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise" (para 87) and referred to the right to "informational self-determination".

With regard to the balancing exercise the ECtHR noted that fair balance has be struck 'between, on the one hand, the applicants' right to respect for their private life under Article 8 of the Convention and, on the other hand, the radio station's and publishers' freedom of expression and the public's freedom of information under Article 10' (para 89).

The ECtHR emphasized the important role the media plays in a democratic society, which involves reporting on court proceedings. It's crucial that discussions about trial subjects happen beforehand or during the trial, whether in specialized journals, the general press, or among the public. The media not only shares information and ideas but the public also has a right to receive them. Without this, the press couldn't perform its vital role as a "public watchdog". And it's not the Court's job, nor the national courts', to decide how the press should report on a case (i.e. whether including identification details or not) (para 89).

Apart from reporting, the press also serves a valuable role by keeping archives of past news and making them available to the public. The ECtHR underscored the importance of internet archives in preserving and providing access to news and information. These archives are significant for education and historical research since they're easily accessible and often free for the public (para 90).

Eventually the ECtHR listed the criteria relevant for the purpose of striking fair balance in this type of cases. The list includes the following considerations:

– contribution to a debate of public interest;
– the degree to which the person concerned is well known;
– the subject of the news report;
– the prior conduct of the person concerned;
– the content, form and consequences of the publication; and
– where it arises, the circumstances in which photographs were taken (para 95).

It is interesting to see how theses criteria were applied to the particular circumstances of the case at hand.

Contribution to a debate of public interest. In the fact setting of the case, the presence of the disputed reports on media websites when the applicants filed their requests continued to contribute to a broader discourse of general interest, unaffected by the passage of time. While the applicants did not seek deletion but anonymization of the material, the approach to covering a given topic falls within journalistic freedom, with journalists tasked with determining what details, like the full name of the individual involved, are necessary to maintain publication credibility, provided such decisions align with professional ethical standards. However, the obligation to reassess the legality of a report at a later stage, following a request from the individual concerned, poses a risk of press reluctance to preserve such reports in online archives or to omit identifying elements likely to be subject to such requests.

The degree to which the person concerned is well known. While it's true that over time, public interest in the crime decreased, the applicants regained attention when they sought to reopen their criminal trial and engaged with the press. Therefore, they were not merely private individuals unfamiliar to the public eye. The subject matter of the reports, such as the conduct of the criminal trial or attempts to reopen proceedings, had the potential to stimulate debate in a democratic society.

The subject of the news report constituted interest for the general public.

The prior conduct of the person concerned. The applicants' efforts to contest their conviction exceeded the standard legal recourse under German criminal law. Due to their engagement with the press, their desire to avoid public exposure of their convictions through media archives held less significance in this case. Consequently, despite their imminent release, they could no longer reasonably expect the reports to be anonymized or for their online presence to be forgotten.

Content, form and consequences of the publication. The disputed texts provided an objective description of a judicial decision, including certain details about the defendants' lives. However, these details were typical considerations in criminal law proceedings and did not aim to discredit or harm the applicants' reputation. Additionally, the reports' placement on the websites made them unlikely to attract users not seeking information about the applicants, and there was no evidence to suggest a deliberate attempt to redistribute the information. Although the internet's pervasive nature makes information easily accessible, the applicants did not attempt to request search engines to limit the visibility of the material. Furthermore, the court did not address the possibility of less restrictive measures concerning

media organizations' freedom of expression, as this was not raised in previous court proceedings.

Circumstances in which photographs were taken. The disputed photographs lacked any potentially damaging aspects. Moreover, the chances of third parties identifying the applicants were diminished because the photos depicted them as they appeared thirteen years before their release.

Considering all these criteria the ECtHR found no violation of Art 8 of the Convention.

It is also worth mentioning that when deciding on the merits of the case the ECtHR referred (para 62) to distinction between publishers and search engine operators, outlined in the judgment of the CJEU in *Google Spain* case. In particular, the CJEU observed that:

"Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page" (para 87).

It follows from the above that it is conceivable that in some set of circumstances the data subject may have the claim against the search engine operator (to request de-listing of the data from search results) but not against the original publisher (to delete the data altogether). In the case of *M. L. and W. W. v. Germany* the applicants requested anonymization from the original publisher. Probably, had they requested delisting from the search results, they would have better chances to succeed.

9.2. Case of Mediengruppe Österreich GmbH v. Austria[23]

The applicant company, which owns the newspaper Österreich, published an article during the 2016 run-off federal presidential elections discussing the political circles of a presidential candidate, N. H. The article included a photograph of H. S., who had been convicted of neo-Nazi activities in 1995 under the National Socialist Prohibition Act. H. S. had been leading a crime-free life since his release from prison in 1999 and having his conviction removed from his criminal record. Therefore, he decided to sue the applicant. National court ruled that the applicant could not publish H. S.'s photograph if he was referred to as a "convicted neo-Nazi" in the accompanying text. However, H. S.'s claim for compensation for non-pecuniary damage was rejected.

Applicant company lodged and application with the ECtHR alleging that prohibition to publish the image with "convicted neo-Nazi" caption violated Art 10 of the ECHR (Freedom of expression).

To decide the case the ECtHR utilized the same as in the case of M. L. and W. W. v. Germany. But being applied to this fact setting those criteria yielded the opposite conclusion favoring this time the right to be forgotten.

Contribution to a debate of public interest. The article focused on N. H. (presidential candidate) having an office manager, H. S.'s brother, who had past associations with individuals aiming to undermine the Austrian constitutional order. Published during the sensitive period of the 2016 presidential election, it garnered significant public interest due to concerns about the election process and candidates. However, the article did not imply any direct connection between N. H. and H. S., nor did it suggest H. S.'s involvement in the election campaign. H. S. was not the subject of

[23] *Mediengruppe Österreich GmbH v. Austria*, no. 37713/18, 26 April 2022. https://hudoc.echr.coe.int/eng?i=002-13635

the article, and thus, publishing his photograph without a complete context did not contribute to the election debate.

Degree of notoriety of the person affected and subject of the news report. The Court emphasized that individuals expressing extremist views, especially those involved in severe crimes like those prohibited by the Prohibition Act, are subject to public scrutiny. This is particularly true for individuals like H. S., who was a prominent figure in the neo-Nazi scene and a leading member of an organization aiming to undermine the Austrian constitutional order. Despite H. S.'s past notoriety, the article in question was published more than twenty years after his conviction and seventeen years after his release, with no indication that he sought public attention thereafter. The applicant company failed to demonstrate that H. S. remained a person of public interest when the photograph was published. While the Court acknowledged the importance of judicial history regarding neo-Nazis in Austria, it noted that H. S.'s notoriety might have changed over the years. Furthermore, the article did not pertain to H. S.'s criminal proceedings or his role in the election campaign.

The prior conduct of the person concerned. H. S. successfully reintegrated into society after his release from prison and remained free of further criminal convictions. However, the applicant company did not provide any evidence during the civil proceedings regarding H. S.'s activities after his conviction, nor did they substantiate their claim that he was still involved in the right-wing scene.

Method of obtaining the information and its veracity. The applicant company's statement about H. S. being a former convicted neo-Nazi was true, but incomplete. It failed to mention that H. S.'s conviction dated back to 1995, that he had completed his sentence, and that he had no further criminal record. This

information could have been easily verified using the Criminal Record Deletion Act.

Content, form and consequences of the publication. The article did not focus on H. S., and he did not claim any specific consequences resulting from its publication in the domestic proceedings, leading to the dismissal of his damages claim.

Severity of the sanction imposed. The limitation placed on the applicant company was minimal. It wasn't penalized in either civil or criminal cases for the report or the photograph's publication. The company wasn't barred from reporting on H. S. or his past crimes, instead it only couldn't publish his image with the label convicted neo-Nazi. No compensation or fine was given, only reimbursement for the domestic proceedings' costs.

*The lapse of time. T*here was no direct link between H. S.'s past conviction and the article's publication in 2016, as his conviction had already been expunged from his record by then. While acknowledging the gravity of H. S.'s past crime and the importance of reporting on neo-Nazi activities, the ECtHR also emphasized the importance of reintegrating ex-convicts into society and their right to move on from their past after a certain period.

10. Conclusion

In conclusion, the right to be forgotten represents a crucial aspect of the broader right to privacy, particularly in the context of today's digital landscape. It empowers individuals to exert control over their personal information online, offering them the opportunity to manage their digital footprint and shape their online identities.

However, it's important to recognize that while the right to be forgotten is significant, it is not without limitations. When individuals assert this right, it necessitates a nuanced examination to strike a delicate balance between safeguarding privacy and

upholding other fundamental rights, such as freedom of expression and the right to access information.

This balancing act involves a multifaceted consideration of various factors. For instance, the contribution of the information to a debate of public interest must be weighed against the sensitivity of the data and the potential harm it may cause to individuals. Additionally, factors such as the notoriety of the person involved, their prior conduct, and the content, form, and consequences of the publication play a pivotal role in the decision-making process.

Moreover, the passage of time can significantly influence the relevance and impact of the information in question. As circumstances change and societal attitudes evolve, what may have once been deemed relevant or newsworthy may no longer hold the same significance.

By carefully navigating these complexities and considering the diverse array of factors we can ensure that decisions regarding the right to be forgotten are made thoughtfully and in alignment with the principles of fairness, justice, and respect for fundamental rights. In doing so, we can cultivate a digital environment that promotes individual autonomy, fosters informed discourse, and upholds the values of a democratic society.

Theme 2
Implementation of European fundamental values in contract and tort law

European Fundamental Values and Contract Law in the Digital Era

Nataliia Filatova-Bilous*

Abstract: This chapter analyses the possibility of horizontal application of the European fundamental values to contractual relationships in the Digital Era. In the modern digitalized world the practice of contract formation and contract performance as well as the role of contracts in whole have significantly changed. Contract is a new regulator which is used globally by the most powerful online platforms, and thus it often touches upon fundamental human rights of the contracting parties. In this paper it is stated that fundamental values may have horizontal effect and may be applied to contractual relationships arising online. However, their role shall not be overestimated.

Keywords: contract law; online platforms; smart contract; automatized contracts; European Fundamental Values; horizontal effect of human rights; constitutionalization of private law

1. Introduction

Contract law is one of the largest areas of private law, which accumulates the most prominent features of this branch of law: party autonomy, dispositivity, horizontality etc. This area

* *Associate Professor at the Department of Civil Justice, Arbitration and Private International Law of Yaroslav Mudryi National Law University; filatovaukraine@gmail.com*

is deprived of any direct statutory intervention, subordination, and coerciveness since it is wholly based on private initiative. Generally, contracts are the result of self-organization of private persons which are drafted to regulate their relationships within a particular area of collaboration: sale of goods, performance of services, sharing of intellectual property (IP) rights, etc.

In the modern world contracts are considered as one of the most significant and powerful instruments of regulation of relationships between various persons. Although in the Digital Era statutory laws, case law and various state regulations are still very important regulators of various relationships, contracts have occupied not less prominent place. Indeed, in today's world, a contract is a universal tool for regulating various relationships: contracts underlie the use of any Internet source, define the rules for users to join the relevant platform, interact with other users, and outline the consequences of breaching these rules. Contracts are literally becoming omnipresent today, as each of us enters dozens of contracts every day while browsing the Internet without even realizing it.

The most prominent example which reveals the importance of contracts in the Digital Era is that contracts are the main source which the most powerful online platforms having billions of users (so-called GAFAM[1]) use to regulate their relationships between them and their users as well as between their users *per se*. Thus, it turns out that these are not statutory laws, regulations or international conventions which regulate online interactions between billions of people and outlining the framework for fundamental human rights online, but contracts drafted by the platforms and deployed in the form of so-called Terms of Service (ToS)[2]. In the end, we find ourselves in the world where our right

[1] Google, Apple, Facebook, Amazon and Microsoft.

[2] *N. Elkin-Korenand and others, Social Media as Contractual Networks: A Bottom Up Check on Content Moderation,* in *Iowa Law Reiew,* Vol. 107, 2022, p. 1000.

to express our opinion online is determined by the contract with the social media we use, our mental integrity depends on the way online platforms we use deal with harmful content in the contracts they conclude with us and other users, etc. This explains why D. Trump's possibility to communicate with his electorate is not a matter of the First Amendment, but a matter of Twitter's or Facebook's Terms of Services (ToS)[3], why Russian information campaign concerning the war in Ukraine is restricted by Facebook and YouTube, but not by Telegram and TikTok (at least as it could and should be restricted), etc[4].

In these circumstances there appears a need to ensure a balanced and nuanced approach to regulate contractual relationships in the modern digital world. Since contractual and private regulation become more and more influential in the Digital Era, a huge debate concerning the possibility to apply human rights standards to contractual relationships has recently arisen, which stems from a broader debate concerning 'constitutionalization of private law'[5].

In the European Union its primary legislation outlines not only fundamental human rights, but also European fundamental values, which are pointed out in Article 2 of the Treaty on European Union (TEU)[6] and in the preamble to the Charter of Fundamental Rights of the European Union[7]. These are:

[3] S. Macedo, *Lost in the Marketplace of Ideas: Toward a New Constitution for Free Speech After Trump and Twitter?* in Philosophy & Social Criticism, Vol. 48, 2022, p. 951.

[4] N. Filatova-Bilous, *Content moderation in times of war: testing state and self-regulation, contract and human rights law in search of optimal solutions,* in *International Journal of Law and Information Technology*, Vol. 31/1, 2023, p. 47.

[5] T. Barkhuysen & M. L. Emmerik, *Constitutionalisation of Private Law: The European Convention on Human Rights Perspective,* in Tom Barkhuysen & Siewert Lindenbergh (ed), *Constitutionalisation of Private Law,* Martinus Nijhoff Publishers, Leiden/Boston, 2006, p. 54.

[6] Consolidated Versions of The Treaty on European Union and the Treaty on the Functioning of the European Union. OJ 7.6.2016, C 202/01.

[7] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are primarily considered as the ones having a constitutional meaning, i.e. as values on which the European Union is founded and which are shared and respected by all Member States[8]. However, the modern tendencies evidence that concepts which originally were created in the field of public (constitutional) law are now granted a broader scope of application. Thus, it may be presumed that European fundamental values may also be somehow applied to contract law issues in the Digital age. Remarkably, some scholars have already made first steps towards this path of analysis, however, regarding these values in the context of private law in general, not only in the context of contract law[9].

Thus, the aim of this paper is to find out whether European fundamental values may be applicable to contract law issues considering the role of contracts in the Digital Era, and if they may, in which way and how they may help to solve current issues arising in online contractual practice.

2. Contract law in the Digital Era: the main tendencies

It is often stated in the academic literature that Digital Era is a product of the Third Industrial revolution, which is based on high-technological automatized production and innovative products, which became possible with the development of computer technologies and instruments[10]. There are no exact time frames

[8] M. W. Hesselink, *Private law and the European constitutionalisation of values*, in *Amsterdam Law School Legal Studies Research Paper,* Vol. 26, 2016, p. 7.

[9] M. W. Hesselink, *If you don't like our Principles we have Others. On core Values and Underlying Principles in European Private Law: A Critical Discussion of the New 'Principles' Section in the Draft CFR'*, in: R Brownsword, H Micklitz, L Niglia & S Weatherill (eds), *The Foundations of European Private Law*, Hart Publishing, Oxford, 2011, 59–72.

[10] J. Rifkin, *The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World*, Palgrave Macmillan, London, 2011, p. 53

of this Era, however, most of scholars consider that it started in the 70s-80s of the XX century[11].

However, obviously the Digital Era is not homogeneous, but rather this is a rapidly developing phenomenon which gains new features as the technology develops and new innovations appear. This is why there is a widespread opinion that currently we are living in the Digital Era of a new quality – the Era which started in 2010s after the Forth Industrial Revolution (a famous concept introduced by Klaus Schwab)[12]. The so-called "Industry 4.0" is based on the combination of the two groups of technologies: material and digital. Material technologies involve 3D-printing, sensor devices and drones, whereas the main digital technologies are cloud computing, artificial intelligence (AI), Big Data analysis and blockchain[13]. These technologies are usually called disruptive ones, since they have a large influence both on other technologies, and on the economic and social life in whole and lead to their rapid and fundamental transformation[14].

Innovations which constitute a basis for the Digital Era have had a large influence on the law in general and on contract law in particular. The changes brought about by these innovations have primarily touched upon the contracting practice, i. e. the way various actors enter, perform and terminate contracts in practice.

In the Digital Age most of the contracts are concluded online. Naturally, the way they are formed differs significantly from the

[11] M. Castells. *The information age : economy, society and culture,* Blackwell, Oxford, 2010, p. 40.

[12] K. Schwab, *The Fiurth Industrial Revolution,* World Economic Forum, Geneva, 2016, p. 11.

[13] Ch. Bai, P. Dallasega, G. Orzes, J. Sarkis, *Industry 4.0 technologies assessment: A sustainability perspective* in *International Journal of Production Economics*, Vol. 229, 2020, p. 1.

[14] K. Schwab, *The Fiurth Industrial Revolution,* cit., p. 13; Ch. Twigg-Flesner, *Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law*, in De Franceschi A (ed.) *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Intersentia, 2016, pp. 21–48.

way paper-based or oral contracts are formed in practice. In particular, electronic contracts may be concluded without any actual participation of their parties in this process and may be fully delegated to artificial intelligence agents (bots), which may act with varying degrees of autonomy depending on the program parameters[15]. Artificial intelligence agents (bots) become even more widespread in light of the development of the Internet of Things, where various tangible objects are connected to a global network and can exchange information between each other and conclude contracts without any human intervention. For instance, a 'smart fridge' can process information about the products stored in it and order those products that are missing without any special order from the owner[16].

The way contracts are performed in the Digital Era also differs from the way they were usually performed previously. Today the performance may be partially or fully automated. Software license agreements concluded electronically, agreements on providing access to digital content, insurance agreements, etc. – in all these contracts a party that has posted an offer to enter them on the Internet (licensee, contractor, insurer, etc.) does not actually take any action to perform them 'manually': the services under these contracts are provided automatically, once the other party gives the necessary information and pays a certain fee, if any.

Moreover, modern technologies ensure not only automatic, but also autonomous automatic performance of contracts, which cannot be interfered with by any party. For example, the performance of smart contracts is fully automatic and is carried

[15] S. Grundmann, Ph. Hacker, *Digital Technology as a Challenge to European Contract Law – From the Existing to the Future Architecture,* in *European Review of Contract Law*, Vol. 13, 2017, p. 255–293 (2017), p. 272

[16] K. Manwaring, *Emerging information technologies: challenges for consumers,* in *Oxford University Commonwealth Law Journal,* Vol. 17, 2017, p. 289 9

out regardless of the will of the parties. Due to the fact that these contracts are concluded and executed on blockchains – decentralized networks in which no participant has decisive influence and control – no one can interfere with or obstruct the process of their performance[17].

Another evidence of the impact of modern technologies on contractual practice is the emergence of new objects of these relations and a change in the nature of existing ones. In particular, one of the most widespread objects of electronic contracts is digital content – data that is created and provided in digital form, like computer programs, applications, games, music, videos or texts. Compared to traditional objects of contractual relationships (tangible objects), digital content is a rivalrous object that can easily be copied. However, digital content has certain characteristics which are important for users, just like ordinary tangible objects have: this is its functionality (the ability to perform certain functions considering the purpose of its creation), interoperability (the ability to perform certain functions on hardware or software that differs from the hardware or software on which similar digital content is usually used), and compatibility (the ability to use it in a way that is not similar to the use of other objects of the material world)[18].

Another type of objects that have emerged under the influence of digitalization are "virtual" or "digital" assets – objects for which various transactions are carried out on the blockchain. What these objects have in common is that they exist exclusively in the digital environment, cannot have material analogues, and are non-rivalrous. Non-rivalrousness of these objects is what makes virtual assets similar to tangible things. However, their legal nature is very

[17] P. De Filippi, S. Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, 2016, p. 11, URL: https://arxiv.org/pdf/1801.02507

[18] Н. Ю. Філатова-Білоус, *Цифровий контент: поняття, особливості і перспективи правового регулювання*, in *Нетипові об'єкти*, І. В. Спасибо-Фатєєва (ed.), ECUS, Харків, 2022, p. 166.

special, and the biggest question about them is how they shall be classified: as digital things, rights *in personam* or as third category of things[19]. This issue has not been fully resolved at the legislative level yet.

In addition to the fact that technology has led to the emergence of new objects, it has also transformed the nature of previously existing ones. This applies to data (both personal and non-personal). For example, in the modern economy, data plays an extremely important role: it is used for the development of software products, marketing strategies, for "training" artificial intelligence, and for machine learning[20]. Thus, data and data sets have become an economic good and even a commodity having a significant property value. Therefore, today data is a transferable good for which various companies and natural persons bargain and conclude contracts. This change in the nature of data is a revolutionary one, especially considering personal data: previously they were understood as an information inextricably linked to an individual which could be transferred anyhow[21].

These and other peculiarities of contracting practice in the modern world have caused significant changes in the concept of the contract and in the approaches to understand its nature. In this regard two opposite tendencies have appeared during the last couple of decades.

On the one hand, there is a huge debate concerning so-called "death of contract law". This academic discussion originated in the

[19] Н. Ю. Філатова-Білоус, *Захист прав на віртуальні активи*, in *Право власності: способи захисту крізь призму судової практики*, І. В. Спасибо-Фатєєва (ed.), ECUS, Харків, 2023, p. 345.

[20] N. Purtova, *Property Rights in Personal Data: Learning from the American Discourse*, in *Computer Law & Security Review,* Vol. 25/6, 2009, p. 508.

[21] А. І. Марущак, *Цивільні права на інформацію,* in *Часопис цивілістики,* Vol. 12/3, 2009, p. 33.

middle of 1970s when Grand Gilmore, an American researcher of law, issued his well-known course of lectures "The death of Contract" [22]. Based on the analysis of the significant changes in legal doctrine and case law of the USA which took place in the 1960s (emergence of collective suits, spreading of the doctrine of estoppel in the case law etc.) the researcher tried to prove that contracts were no longer the same as they had been, and thus contract law was slowly going to its end.

During the last decade debates concerning the "death of contracts" have gained more and more attention among scholars. It is said that under the influence of the Digital Era the contract in its classical meaning is in fact dying[23], while the theory of contract law has become a mythology[24].

First, in the modern contracting practice there is an obvious crisis of the basic principle of contract law – principle of its obligatory nature for parties (*pacta sunt servanda*). The main issue of this principle is that contracting parties are obliged to perform a contract because they voluntarily and consciously agreed to take contractual obligations. However, the way most of the contracts are concluded in Digital Era undermines this principle, since parties' consent to enter a contract and to take contractual obligations is usually formal an unconscious[25]. Undoubtedly, most of the contracts we conclude online and offline are contracts of adhesion and boilerplate agreements. Since ordinary Internet users cannot influence the content of these contracts, they almost never read them, while to conclude them, they merely need to do the simplest act – to click, to scroll, etc.

[22] G. Gilmore, *The Death of Contract,* Ohio State University Press, Columbus, 1974, p. 1.

[23] F. G. Snyder, A. M. Mirabito, *The Death of Contracts*, in *Duquesne Law Review*, vol. 52/2, 2014, p. 348.

[24] J. MacLean, *The Death of Contract, Redux: Boilerplate and the End of Interpretation*, in *Canadian Business Law Journal*, vol. 58/3, 2016, p. 4.

[25] J. MacLean, *The Death of Contract, Redux: Boilerplate and the End of Interpretation*, cit. p. 4

Second, in the Digital Era most of the contracts do not in fact contain any obligation which their parties have to perform purposefully and consciously. Modern technologies have created wide opportunities to make contract performance wholly or partly automated, so parties are no longer obliged to do anything on their own. Automated contracts are widely used by various platforms (streaming services, social media etc.), financial service providers (banks and others) since they help to save time and money to perform contracts 'manually'. Moreover, modern smart contracts allow contract performance to be not only automated, but also autonomous: since they are usually deployed on public blockchains where nobody can alter any record, the way they are performed depends to a high extent on the code they contain, but not on the acts or decisions of their parties[26].

On the other hand, there is a large academic debate on a new quality and a new role of contracts and contract law, which we face in the Digital Era. Back in the end of the 1990s scholars admitted that contracts started to play more and more significant role in the regulation of various social relationships. For the first time the contract was considered as a source of law, but not only as a private instrument[27]. The main reason for this were technological revolutions and the changes they caused in the world economy and social life. Globalization of the economy has led to the decrease of the role of the states in the regulation of various relationships. Meanwhile, constant transformation of modern economy under the influence of innovations and technologies requires more flexible mechanisms and instruments of regulation, and the contract is the most effective and widespread among them[28].

[26] A. Savelyev, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*, in *Information & Communications Technology Law*, Vol 26/1, 2017, p. 17.

[27] K. P. Berger, *The Creeping Codification of the New Lex Mercatoria*, Kluwer Law International, Boston, 1999, p. 108.

[28] F. Galgano, *The New Lex Mercatoria,* in *Annual Survey of International & Comparative Law*: Vol. 2/1, 1995, p. 99.

Strengthening the role of the contract can be seen in various areas of modern social life. It has become possible since the contract itself in the Digital Era has changed dramatically and took up new features which it lacked previously.

First, modern contracts usually contain very detailed terms, whereas the number of vague terms is minimal[29]. This allows to avoid ambiguities in interpretation and application of contract terms by contracting parties and to ensure contract performance without any third party (a judge or an arbiter) if some of its parties fails to perform it duly.

Second, as mentioned above, contracts in the Digital Era are very often automatized, which allows to minimize the need to rely on coercive state mechanisms to make parties duly perform them. Most of the contracts concluded online are drafted in a way that makes it impossible even to enter a contract if you are not able to perform it (if you do not have money on your account, lack instruments to provide an online service etc.)[30].

Third, even if a dispute between parties arises, modern contracts have a wider range of instruments to resolve them, which involve a lot of alternative dispute resolution mechanisms (ADR). These are mediation, arbitration, online dispute resolution (ODR), which purport to resolve legal disputes based on the compromise between contracting parties[31]. Noticeably, in the European Union implementation of these mechanisms is mandatory: according to the Directive 2013/11/EU on alternative dispute resolution for consumer disputes consumers regardless of the state of their habitual residence are guaranteed the right to lodge complaints on businesses to ADR entities created in the

[29] F. G. Snyder, A. M. Mirabito, *The Death of Contracts,* cit., p. 368.

[30] E. Mik, *Contracts in Code?* In *Law, Innovation and Technology*, Vol. 13/2, 2021, p. 485.

[31] C. V. Giabardo, *Private Justice: The Privatisation of Dispute Resolution and the Crisis of Law*, in *Wolverhampton Law Journal*, 4, p. 17.

EU, which are obliged to ensure a fair due procedure of hearing of these complaints[32].

Besides ADR, modern contracts largely rely on other mechanisms facilitating their due conclusion and performance. The most prominent among them are rating systems which are nowadays introduced and used by lots of websites, mobile applications and online platforms. Using these systems a person who is not satisfied with the quality of goods, services or with the content posted by other users has an opportunity to complain on them and to leave a negative comment. This evaluation is visible for other users and is publicly accessible, which can badly influence the other user's reputation. In the market economy with its high level of competition rating systems allow not only to defend rights, but also to prevent their violation[33].

As mentioned previously, there are a lot of factors which led to the strengthening of the role of contracts in the Digital Era. Besides globalization and rapid transformation of the global economy, not less important in this process is the factor of platformization of social relationships based on the Web 2.0 online communication. While initially Internet communication and interaction between users was to a high extent deprived of an order and monitoring by some online structures, modern Internet is well-structured and segmented. Internet users communicate and interact with each other via various online platforms (like Facebook, TikTok, X etc.) which are extremely powerful and giant entities usually called 'digital sovereigns'[34]. From economic perspective these entities

[32] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) *OJ L 165,* 18.6.2013, p. 63–79.

[33] V. Mak, *Legal Pluralism in European Contract Law (Oxford Studies in European Law)*, OUP, Oxford, p.147.

[34] I. Pretelli, *A Focus On Platform Users as Weaker Parties*, in A. Bonomi/G. P. Romano (eds.) *Yearbook of Private International Law, Volume XXII,* Verlag Dr. Otto Schmidt, 2021, p. 203.

are subject to a "scale effect": the more users they have, the more attractive they are for other users, which causes endless increase of the number of their uses[35]. This explains why modern online platforms are so large and how powerful in fact they are.

From the legal perspective online platforms are 'contractual architectures': their relationships with their users as well as the relationships between their users *per se* are based on contracts[36]. Noticeably, all of them are contracts of adhesion drafted by a platform itself and offered for the persons who want to become platform users on a 'take it or leave it basis'. Usually these contracts are called "Terms of Use" (or "Terms of Service"). These ToS regulate a large number of issues: from the way users should choose their names and avatars on the platform to the way they should express their thoughts and feelings online, from the way users should pay for the advertisement they want to place online to the way their personal data is used and processed. In the end, ToS tackles a lot of issues related to the fundamental rights of their users, like freedom of expression, right to respect for human dignity, right to mental integrity etc. Based on these rules platform operators may legitimately make decisions which have a huge influence both on particular persons and on the society as a whole. This can be well demonstrated by the Facebook's and Twitter's decision to terminate Donald Trump's accounts[37], termination of Russian bloggers' accounts on YouTube[38], etc.

Thus, we can observe a paradox of the modern role of a contract. On the one hand, it remains a private instrument which regulates

[35] A. Hein, M. Schreieck, T. Riasanow, D. S. Setzke, M. Wiesche, M. Böhm, H. Krcmar, *Digital platform ecosystems* in *Electronic Markets*, Vol. 30/1, 2020, p. 92.

[36] T. R. de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU,* in *Italian Law Journal*, Vol. 3/1, 2017, p. 150.

[37] S. Macedo, *Lost in the Marketplace of Ideas,* cit., p. 510.

[38] N. Filatova-Bilous, *Content moderation in times of war: testing state and self-regulation, contract and human rights law in search of optimal solutions,* cit., p. 50.

relationships between no more than two or several persons. However, on the other hand, this is a powerful regulator, since when there are a billion of persons, whose relationships between each other and with a platform are regulated in the same way by the same contracts, the contract becomes a powerful regulator, a law for all these persons. Noticeably, at some point a contract may become even a more powerful instrument than the statutory law. First, it can extend its scope beyond statutory borders when it regulates relationships between Internet users from all the globe. Statutory laws generally do not have this power since the borders of their scope usually depend on the borders of a state where they were adopted. Second, as a private instrument a contract is not subject to constitutional control, unlike statutory laws. Thus, contractual provisions are not subject to any checks from classical constitutional or rule of law perspectives. Finally, contractual provisions are more flexible than statutory ones, since they do not have to go through all the parliamentary formalities before being passed.

In this context there is a need to look for new possible 'checks and balances' in the Digital Era considering the new role of private regulation and contracts.

3. The concept and the essence of the European Fundamental Values

European values are outlined in the basic normative documents of the EU: in the Treaty on the European Union (TEU) (now introduced in the consolidated version with the Treaty on the Functioning of the EU (TFEU))[39] and in the Charter of Fundamental Rights of the European Union (CFREU)[40]. According to article 2 of

[39] Consolidated Versions of The Treaty on European Union and the Treaty on the Functioning of the European Union. OJ 7.6.2016, C 202/01.

[40] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

the TFEU the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. In its turn, the CRFEU in its preamble says that the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on the principles of democracy and the rule of law.

Thus, the difference is minor, but it still exists. While the TFEU lists six fundamental values, the CFREU mentions four values, adding solidarity as a value, while democracy and the rule of law are mentioned as basic principles, but not as values.

Despite this difference, the main idea is the same: to bring the fundamental issues on which the EU is founded forward and to provide them with normative power. As mentioned in the academic literature, the EU stands for the plurality of values, and its primary legislation provides a 'basket' (or a 'bouquet') of values, instead of focusing on some of them[41]. In particular, it puts together types of values, which are usually perceived as being opposite to each other: while human dignity, freedom, democracy, and respect for human rights are liberal values, solidarity and equality are social values[42].

The essence of each value is uncovered in the CFREU, which contains seven Titles, each of which is named after each value.

In particular, Title 1 is named *"Human dignity"* and involves several provisions: one on human dignity *per se* and other four – on particular human rights (right to life, right to the integrity of a person, prohibition of torture and inhuman or degrading treatment or punishment, and prohibition of slavary and forced labor)[43]. In

[41] M. W. Hesselink, *Private law and the European constitutionalisation of values,* cit., p. 15.

[42] X. Groussot, E. Karaeorgiou, *Solidarity and the Crisis of Values in the European Union*, in Nordic Journal of European Law Special Issue, Vol. 6/2, 2023, p. 30.

[43] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

the academic literature human dignity is described as being 'closely linked to the inherent worth of individuals and the protection thereof, so it is shaped differently than other fundamental rights'[44]. Human dignity 'cannot be limited or restricted, not even on the grounds of protecting other fundamental rights', while fundamental rights' purpose is to secure human dignity'[45]. Thus, the rights mentioned in Title I of the CHREU (right to life, right to the integrity, etc.) serve for the protection of human dignity, while human dignity itself is more than the right – it is an intrinsic feature of a human being.

Freedom is uncovered in Title II of the CHREU, which involves basic provisions on human rights: right to liberty and security, respect for private and family life, protection of personal data, right to marry and right to found a family, freedom of thoughts, conscience and religion, freedom of expression and information, freedom of assembly and association, freedom of arts and science, and right to education[46]. From the philosophical perspective, freedom *per se* is seen as a "valuable issue as such, i.e. which has value independently of the value of the particular things it leaves us free to do"[47]. Meanwhile, rights that are mentioned in the CHREU in the Title called "Freedoms" disclose various aspects of the freedom as a whole: although each right is defined quite broadly, they all touch upon some aspect of the freedom as such. Even the right to liberty and security is not a general notion outlining the measures of freedom as such, but relates only to a very specific

[44] N. Bermejo, *Fundamental Rights and Horizontal Direct Effect under the Charter*, in: C. Izquierdo-Sans, C. Martínez-Capdevila M. Nogueira-Guastavino (eds), *Fundamental Rights Challenges*, Springer, Cham, p. 14.

[45] N. Bermejo, *Fundamental Rights and Horizontal Direct Effect under the Charter,* cit. p. 14.

[46] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

[47] I. Carter, *The Independent Value of Freedom*, in *Ethics,* Vol. 105/4, 1995), p. 845.

aspect of human liberty, the freedom of bodily movement in the narrowest sense of arrest and detention[48].

Equality is defined through the provisions of Title III, which contains articles on equality before the law (article 20), non-discrimination (article 21), cultural, religious and linguistic diversity (article 22), equality between women and men (article 23), the rights of the child (article 24), the rights of the elderly (article 25), and integration of persons with disabilities (article 25)[49]. In some publications equality is considered as a fundamental human right, i.e. a right to an equal treatment or simply a right to equality[50]. However, in the CRFEU and in other EU acts (e.g. in the Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation) it is called "a value" or "a general principle of EU law"[51]. In this second meaning equality is not merely a right, but a guarantee that fundamental human rights will be respected and protected regardless of any specific characteristic of a person (her gender, race, age, etc.). Thus, equality is an issue which facilitates and ensures human rights protection in its broad meaning, and for this reason it is a value on which the EU law is based. The essence of equality is uncovered through various provisions: general non-discrimination, diversity, and equal rights of persons belonging to various social, cultural and religious groups.

Solidarity is another value mentioned in the TFEU and CRFEU. Solidarity is a broad concept having various facets: it characterizes both mutual commitments of individuals within the society and

[48] Commentary of the Charter of Fundamental Rights of the European Union. EU Network of Independent Experts on Fundamental Rights, 2006, p. 67, URL: https://sites.uclouvain.be/cridho/documents/Download.Rep/NetworkCommentaryFinal.pdf

[49] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

[50] M. Nowak, *Civil and political rights*, in J. Symonides (ed), *Human Rights: Concept and Standards*, UNESCO Publishing-Ashgate, Aldershot 2000, p. 98.

[51] T. Papadopoulos, *Criticizing the horizontal direct effect of the EU general principle of equality*, in *European Human Rights Law Review*, Issue 4, 2011, p. 440.

mutual commitments of state and civil institutions[52], it can manifest itself at the intrastate and at the interstate level[53].

At the interstate (global level) solidarity is a characteristic of relations between states, which is based on mutual commitments, goals, and help[54]. In this meaning this concept is used in the TFEU and in the TEU where it sets rules on what the relationships between Member States shall be like: Member States shall support the Union's external and security policy actively and unreservedly in a spirit of loyalty and mutual solidarity (article 11 of the TEU), shall act in solidarity in the context of the establishment and functioning of the internal market and with regard for the need to preserve and improve the environment (article 194 of the TFEU), act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster (article 222 of the TFEU).

At the intrastate level solidarity is associated with constitutional endorsement of the welfare-state model, and with the recognition of social rights, and thus primary imposes obligations upon the state[55]. In this vein the concept of solidarity is defined in the CRFEU. Its Title IV which is named "Solidarity" contains several provisions most of which are provisions of social rights (workers' right to information, right of collective bargaining, right of access to a free placement service etc.), while other provisions come down to imposing obligations on the Member States and the Union as a whole (prohibition of child labor, social security and social assistance, environmental, consumer protection, etc.)[56].

[52] D. Miller, *Solidarity and Its Sources*, in K. Banting, W. Kymlicka (eds.) The Strains of Commitment: the Political Sources of Solidarity in Diverse Societies, Oxford Academic, Oxford, 2017, p. 62–63.

[53] T. H. Brandes, *Solidarity as a Constitutional Value*, in Buffalo Human Rights Law Review, Vol. 59, 2021, p. 81–85.

[54] T. H. Brandes, *Solidarity as a Constitutional Value*, cit., p. 84.

[55] T. H. Brandes, *Solidarity as a Constitutional Value*, cit., p. 81.

[56] Charter of Fundamental Rights of the European Union. *OJ C 326, 26.10.2012, p. 391–407.*

Another value which is mentioned in the TFEU (however, not mentioned in the CHREU) is the *respect for human rights*. This category is extremely broad and encompasses both human rights themselves and guarantees of their protection as they are drawn up in various international and European conventions and other legal documents. Basic provisions concerning this value are set up in Article 6 of the TFEU. What follows from it is that: a) fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) shall constitute general principles of the Union's law; b) the EU as such accedes to the ECHR, which means that not only Member States, but the EU in whole takes on the obligations in the field of human rights protection imposed by the ECHR; c) the EU recognizes the rights, freedoms and principles set out in the CHREU which has the same legal value as the Treaties[57].

As a value and a general principle of the Union law the respect for human rights relies on the obligation of the Member States and of the Union to guarantee and protect human rights. These obligations are established by various international treaties and other documents, in particular, in the ECHR and CHREU. Besides obligations to respect and to protect particular rights and freedoms (right to life, freedom of expression, freedom of association etc.) the ECHR imposes general obligations on all its Contracting Parties to secure to everyone within their jurisdiction the rights and freedoms. This involves two types of obligations: i) a negative obligation to refrain from actions incompatible with the Convention (i.e. an obligation not to violate human rights); ii) a positive obligation to guarantee respect for the rights and freedoms secured under the Convention (i.e. not to let other persons violate human rights

[57] Consolidated Versions of The Treaty on European Union and the Treaty on the Functioning of the European Union. OJ 7.6.2016, C 202/01.

within the countries' jurisdiction)[58]. Thus, the EU itself (including all its institutions) and its Member States are bound by the ECHR[59] and thus carry out both positive and negative obligations in their jurisdictions. Besides ECHR, the EU and its Member States shall observe the provisions and principles set up in the CHREU when implementing the Union law (article 51 (1) of the CHREU). The Charter guarantees that the protection it provides may never fall below that provided by the ECHR, but may go beyond the level of protection provided by the Convention[60]. The fact that the EU and its Member States are bound by obligations imposed by the ECHR and the CHREU means that (i) the EU law and the law of its Member states shall be drafted with the human rights standards in mind and shall seek to protect them; (ii) the EU and the Member States' law shall be interpreted and applied taking into account the obligations in the field of human rights protection.

Finally, there are values of *democracy* and the *rule of law*.

Democracy as a value and as a principle is unfolded in the Title II of the TFEU and relates to the way the Union institutions and bodies are formed and the way the EU citizens may participate in their formation. Article 10 sets up that the functioning of the Union shall be founded on representative democracy. Citizens are directly represented at Union level in the European Parliament. Member States are represented in the European Council by their Heads of State or Government and in the Council by their governments, themselves democratically accountable either to

[58] Guide on Article 1 of the European Convention on Human Rights. Council of Europe/European Court of Human Rights, 2022, p. 25.

[59] K. L. Mathisen, *The Impact of the Lisbon Treaty, in Particular Article 6 TEU, on Member States' Obligations with Respect to the Protection of Fundamental Rights,* in *University of Luxembourg Law Working Paper*, No. 2010–01, URL: https://ssrn.com/abstract=1650544, p. 35.

[60] K. L. Mathisen, *The Impact of the Lisbon Treaty, in Particular Article 6 TEU, on Member States' Obligations with Respect to the Protection of Fundamental Rights,* cit., p. 28.

their national Parliaments, or to their citizens. Every citizen shall have the right to participate in the democratic life of the Union[61]. Thus, democracy is a characteristic of the political process in the EU and its basic principle.

The rule of law is not expressly defined in the TFEU or in the CHREU, however, obviously this broad and fundamental concept relies on the way it is outlined in other international legal documents. Basic among them for the European continent is the ECHR and the European court's of human rights (ECtHR) case law where this concept has been determined for many times and from various angles. As mentioned in the ECtHR judgements, the rule of law is a concept inherent in all the Articles of the Convention[62], which allowed scholars to conclude that the rule of law is a basis of the conventional system of human rights protection providing the ECtHR with an ability to guarantee not theoretical or illusionary rights, but their practical and effective application[63]. The rule of law is a multifaceted concept which involves a number of aspects. T. Tsuvina outlines four of them: 1) legality – only the law may be a basis for a state's infringement into human rights and only the law may outline measures of admissible interference with human rights; 2) legal certainty – the application of laws shall be foreseeable for a person to whom the law is applied; 3) fair trial – any human rights infringement by state bodies shall be controlled by courts, and every person shall have a right to court under article 6 of the ECHR; 4) respect for human rights – a substantial element of the rule of law

[61] Consolidated Versions of The Treaty on European Union and the Treaty on the Functioning of the European Union. OJ 7.6.2016, C 202/01.

[62] European Court of Human Rights Judgement. Amuur v. France, App. Nos. 19776/92 (1996).

[63] J. Meyer-Ladewig, *The Rule of Law in the Case-Law of the Strasburg Court*, in H.-J. Blanke and S. Mangiameli (eds.) *The European Union after Lisbon*, Springer, Berlin, 2012, p. 236.

interpreted as a rule of human rights and freedoms, priority of their protection over other aims[64].

As the analysis shows, values outlined in the EU primary legislation are extremely broad and multifaceted concepts. Most of them (equality, dignity, solidarity, freedom) involve various fundamental human rights, however, the essence of these values does not come down merely to the combination of these rights. Rather the values combine both human rights and the way they shall be protected and guaranteed in the EU and by each Member State. The values of democracy and the rule of law, on the other hand, are those pillars which make human rights protection possible as such. They are the most important guaranties of respect for human rights in the EU and in every Member State.

Another important characteristic of fundamental values is that they are shared by all Member States and across the whole Union. However, it also means that the territorial scope of values is limited with the borders of the EU. Values are not only legal concepts, but also culturally and morally dependent categories, and for them to be shared by some societies it is crucial to have a link with these societies.

4. European fundamental values and modern contract law: is the horizontal effect possible?

Values outlined in the EU law as well as human rights traditionally are considered as constitutional concepts[65]. However, the most recent tendencies in academic discussion evidence that this approach is no longer axiomatic. There is a general academic debate on the constitutionalization of private law, which reflects the increasing

[64] Цувіна Т. А. Принцип верховенства права у практиці Європейського суду з прав людини. Часопис Київського університету права. 2019. № 4. С. 374–376.

[65] M. W. Hesselink, *Private law and the European constitutionalisation of values,* cit., p. 1.

influence of fundamental rights in relationships between private parties[66]. This constitutionalization currently refers primarily to human rights and comes down to providing human rights standards with horizontal effect, i.e. with the possibility to be applied not only to relationships with the states, but also to the ones between private parties[67]. As is known, obligations in the field of human rights protection are traditionally imposed on the states. However, currently it is often discussed that these are not only states who are responsible for human rights protection, but private persons as well. This debate often falls within the academic discussion on the responsibilities of businesses concerning respect for human rights[68]. Noticeably, this idea has inspired the international community to review the classical approaches to human rights and gave birth to the U. N. Guiding Principles on Business and Human Rights[69].

The debate concerning business and human rights has paid special attention to modern issues brought about by digitalization and platformization. A U. N. special rapporteur on the promotion and protection of rights to freedom of expression, David Kaye, in his well-known report in 2018 specifically stressed the need for modern online platforms to comply with international human rights standards when introducing their policies and carrying out their activities towards their users (i.e. in private relations with their users)[70].

---

[66] J. M. Smits, *Private law and fundamental rights: a sceptical view,* in T. Barkhuysen & S. Lindenbergh (eds.) *Constitutionalisation of Private Law,* Martinus Nijhoff Publishers,Leiden/Boston, 2006, p. 10.

[67] Б. П. Карнаух, *Захист власності Європейським судом з прав людини і горизонтальний ефект* in *Право України*, Issue 5, 2021, p. 149.

[68] O. Uvarova, *Business and Human Rights in Times of Global Emergencies: Comparative Perspective,* in *Comparative Law Review,* Vol. 26, 2020, p. 225.

[69] Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework (*United Nations*, 2011). URL: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[70] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 70, U. N. Doc. A/HRC/38/35 (Apr. 6, 2018).

In academic debate the idea of horizontal effect of human rights has been applied to various areas of private law, in particular, to contract law. It has been stated that "fundamental rights do not merely influence contract law as a conceptually distinct and autonomous category, [but also] govern contract law, thereby enjoying priority over its internal principles of justice"[71]. This approach towards extrapolating human rights standards to contract law has been found fruitful for addressing the challenges which arise in modern contract law and in contractual practices between platforms and their users. Human rights standards can serve as an instruction providing precise criteria for distinguishing acts done by platforms vis-a-vis their users in good faith from those that are done in bad faith. A platform complies with the principle of good faith within its contractual relationships with its users if its actions have been legal (the platform's contracts with its users precisely identify grounds to impose restrictions), legitimate (restrictions have had sufficient grounds), proportional (there have been no softer measures capable of combating harmful consequences), and its users have been provided with due process guarantees and remedies to object its decision[72].

Application of human rights to contractual relationships may be helpful, in particular, in the following aspects: i) it provides for an opportunity to distinguish enforceable contractual clauses from non-enforceable: if the clause was not duly negotiated with the user or is manifestly unfair, discriminating etc. it may not be enforced against the user; ii) it helps to apply contractual provisions fairly and in good faith and allows to distinguish harmful practices against Internet users; iii) it provides for an opportunity

[71] O. Cherednychenko, *Fundamental Rights, Contract Law and Transactional Justice*, in *European Review of Contract Law,* Vol. 17/2, 2021, p. 133.

[72] N. Filatova-Bilous, *Content moderation in times of war: testing state and self-regulation, contract and human rights law in search of optimal solutions*, cit., p. 68.

to find appropriate and effective remedies to protect the rights which have been violated because of unlawful or harmful contract terms, etc.

All these conclusions have been formulated in various publications with respect to horizontal effects of human rights and its benefits. One of the reasons why it gained much support among scholars is that the doctrine of human rights is well-developed and consistently applied by international bodies, in particular, by ECtHR. Human rights are not only a set of various legal opportunities granted to persons by the law – this is a set of well-balanced and well-structured human rights standards (legality, legitimacy, proportionality, due process etc.), which help to outline the exact measure of what a person can or cannot do and to which extent other persons (primarily the state) may interfere with these possibilities. Considering contract law, these standards help to outline an admissible interference of one party into the rights of the other party and to balance the rights belonging to different parties when these rights collide.

But what about fundamental values: can they be applied to modern contractual relationships horizontally just like fundamental rights?

The concept of fundamental values is not that well-developed as the concept of fundamental human rights is. Moreover, it is often criticized by scholars: they are rather vague, and their legal enforceability is questionable since they are established to outline what is *valuable*, but not was its *lawful* or *permissible* (emphasis added)[73]. Applying fundamental values to private, in particular, contractual relationships, is much more challenging. First, unlike human rights, no criteria have been developed in academic literature or in case law on the way values shall be applied to public

[73] M. W. Hesselink, *Private law and the European constitutionalisation of values,* cit., p. 4.

relationships, more so – to private ones. Thus, unlike human rights which can enrich case law in private disputes with the standards of legality, legitimacy, proportionality etc., values are not able to provide such an enrichment. Second, it is very questionable whether values may be applied horizontally since the EU primary legislation addresses them to the Member States and the EU in whole obliging these public entities to promote values (article 13 of the TEU), safeguard them (article 21 (2) of the TEU), respect them (article 49 of the TEU) etc.

However, the concepts being very close to European fundamental values have already been applied horizontally in the case law. The most prominent case in this regard is *Werner Mangold v Rüdiger Helm* heard by the European Court of Justice (ECJ), where the court by and large came to the conclusion that the fundamental principle of equality and non-discrimination in labor relationships (in particular, non-discrimination on the grounds of age) is capable of horizontal effect and employers should comply with it while hiring employees[74]. Although this case concerned a narrower issue and primarily came down to the applicability of principles set up in the Directive 2000/78 establishing a general framework for equal treatment in employment and occupation, the conclusion formulated by the ECJ is worth analyzing in a broader context for at least two reasons. First, equality and non-discrimination are not only principles of the Directive at hand, but also a European fundamental value of equality outlined in article 2 of the TEU. Second, as the case shows, this principle/value can be applied in private disputes like the one at hand and, presumably, in other types of private disputes as well.

[74] Judgment of the Court (Grand Chamber) of 22 November 2005, Werner Mangold v Rüdiger Helm, Case C-144/04, ECLI:EU:C:2005:709; T. Papadopoulos, *Criticizing the horizontal direct effect of the EU general principle of equality,* cit., p. 438.

Thus, it seems incorrect to deny any possibility to apply fundamental values to private, in particular, contractual disputes. The fact that there are some difficulties with their application does not evidence that this is impossible at all. To answer the question whether they are applicable we need first to find out whether this application may be helpful and useful in practice, i.e. whether values are valuable in practice of solving private disputes.

The main strength and simultaneously the main weakness of fundamental values as a legal concept is that their main function is *to evaluate* various phenomena: cases arising in practice, acts done by various actors, circumstances in which they are done, etc. This feature of values may be helpful since it provides state bodies, independent arbiters, mediators, other entities authorized to resolve disputes, and private parties with an opportunity to distinguish what is 'good' from what is 'bad' or what is 'admissible' from what is 'inadmissible'. Moreover, the fact that the EU sets up its values in its primary legislation means that the value framework is commonly shared by all Member States and their public and private actors, which allows to regard every practical case through the same 'value lens'. This feature acknowledges that the application of values may be indeed helpful in a large number and variety of cases – not only in cases involving public entities, but also in private cases, since both of them come down to the evaluation of acts done by these or that persons.

The analysis of applicability of fundamental values seems to be much more productive when each value is regarded separately since each of them has its own framework system of evaluation.

The *value of dignity* as mentioned in the previous section is a concept outlining inherent worth of the individual which is inalienable and unrestrictable and which is ensured by a set of human rights: right to life, right to the integrity of a person, etc. In the modern contractual practice, the issue of dignity arises very

often, especially when it collides with the rights and freedoms of other persons, e.g. the freedom of expression. A simple example is when some users of a social media platform send abusive messages to the other user (messages containing bullying, flashing images to make a person with epilepsy suffer harm, etc.), and a platform operator needs to react somehow. On the one hand, any platform operator's act will be done within a contractual relationship with each particular user, thus, it will have a pure contractual nature. However, on the other hand, in the end it will obviously go beyond particular contracts and will touch upon a fundamental value – a value of dignity of the aggrieved user. In these circumstances the platform operator becomes an arbiter who, acting within contractual relations, needs to protect its user's dignity. Modern legislations partly help to resolve this uneasy task: for instance, Online Safety Act adopted in the UK regards sending threatening materials, flashing images, bullying content etc. as an offence and allows platform operators to remove content of this type and to impose other restrictions for the users sharing it[75]. However, many types of harmful content remain uncovered, thus, platform operators need to decide on their own how to act in these cases. The value of human dignity and the human rights on which it relies may be helpful in this regard.

Another value is *freedom*, which is an extremely broad category involving various human rights (freedom of speech, freedom of association, of movement, etc.). In modern contract law the need to apply this value may arise in various circumstances, however, the most widespread case where it arises is where a user of a social media platform shares information, but whether this is lawful and harmless is very disputable. This occurs, inter alia, where the information contains fakes, hate speech or may otherwise be

[75] Online Safety Act 2023. URL: https://www.legislation.gov.uk/ukpga/2023/50/contents

harmful. In these circumstances the platform operator often needs to react somehow, and again any of its acts will be done within the contractual relationship with the user who shared the content, but obviously in the end these acts will result in resolving difficult issues concerning freedom of expression and sometimes – human dignity. In this case the operator has to evaluate the information shared and make a balanced decision. Again, modern legislation provides clear rules of how the operator shall act: the Digital Services Act of the EU, for example, allows operators to remove the unlawful content and apply other sanctions (like termination of the account) to the users[76], but not always does the content shared online qualify as unlawful, although its harmfulness is indisputable. Thus, the platform operators again need to resolve these cases based on more flexible criteria, and the value of freedom together with human rights which it involves may be helpful.

The value of equality presumes non-discrimination on any specific characteristic which a person has. As mentioned above, there already exists case law where this value (although in a narrower meaning) has been applied to private relationships. In modern contractual relationships this value may also be applicable and helpful. In particular, since most of the contracts which are concluded online are contracts of adhesion and contracts based on a so-called public offer, it is important to ensure equality and non-discrimination at the stage of conclusion of these contracts. In particular, if a transaction platform provides businesses with an opportunity to sell their goods or provide their services, it is important to ensure that all the business who wish to join the platform will have equal possibilities to do this and to enter a contract with the platform operator. Partially this is guaranteed by

[76] 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) (Text with EEA relevance) *OJ L 277, 27.10.2022, p. 1–102.*

the provisions of the Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services which purports to ensure equal and fair treatment of business users offering their goods and services online[77]. However, its provisions do not comprehensively cover all the issues which may arise in practice, in particular, they do not cover conclusion of the contracts between platforms and business users, where the equality and non-discrimination is of a particular importance. Here the value of equality itself may be important and helpful.

Solidarity is a value characterizing mutual contributions of various actors into the commonwealth and well-being. Although this value relates mostly to state bodies and institutions, in a broad meaning it also concerns private actors and entities. Considering peculiarities of contract law in a modern digitalized world it seems that this value may also be applicable to contractual cases. In particular, since modern Internet is segmented by various online platforms each of which is a 'contractual architecture' (i.e. a set of contracts between various users and a platform itself), mutual commitments are crucial to ensure a balance in these architectures and systems. For instance, users of online platforms shall not place illegal content, while social media platforms shall create for their users an opportunity to notify them about illegal content placed by other users. Meanwhile, other users who notice presumably illegal content shall notify the platform about it, but the notification shall not be groundless. These obligations are partly mentioned in the modern EU legislation, in particular, in article 16 and other articles of the Digital Services Act of the EU[78]. However, the Act focuses

[77] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) OJ L 186, 11/07/2019, p. 57–79.

[78] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) OJ L 186, 11/07/2019, p. 57–79.

primarily on the platforms', but not users' obligations. Thus, the value of solidarity may help to derive the mutual platforms' and users' obligations which follow from their contractual relationships and to depict the whole image of how these obligations turn into mutual commitments and contribute to the balance of interests and rights on the platform in whole.

The values of *rule of law* and *respect for human rights* are indisputably interconnected and complement each other: human rights are illusory without the rule of law, whereas the main role of the rule of law is to ensure an effective protection of human rights. Both concepts rely on a well-developed case law and doctrine which have elaborated criteria and standards of their application. As for the human rights, there is a set of standards which in practice provide an opportunity to distinguish cases where their infringement is justified and where it is not: these are legality (whether there is a law which allows to interfere with the right), legitimacy (whether there is a legitimate aim of the infringement), proportionality (whether the infringement is adequate in the circumstances at hand) and a due process (whether a fair procedure has been observed when the right has been infringed)[79]. The rule of law as has already been mentioned relies on legality, legal certainty and fair trial[80]. Obviously, the basic concepts of both values (principles) are very common, and what is particularly important is that they can complement other values (freedom, dignity, equality etc.) with more precise criteria and standards, which will ensure their better application in practice.

To the cases stemming from the modern contractual practice these criteria and concepts seem to be applicable as well. For

[79] B. Sander, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation, in Fordham International Law Journal, Vol. 43, 2020,* p. 971.

[80] Т. А. Цувіна, *Принцип верховенства права у практиці Європейського суду з прав людини*, cit., p. 374–376.

instance, if we refer to the case where a platform user posts information which is harmful for other users (like hate speech or disinformation), we can see that here a platform operator needs to make an uneasy decision concerning the content at hand: whether to remove it or to leave as it is, whether to block the users' access to the account or to block the possibility of other users to see the content, etc. As mentioned above, modern EU legislation (in particular, the Digital Services Act) provides platform operators with some instructions for these cases, however, this area remains within the contractual relationships and thus no statutory provisions can dictate how the platform shall act in this or that case. In fact, this uneasy category of cases lies within the platform operator's discretion, although the latter still needs some indicators of what to do and what to decide. These indicators may be found in the concepts of respect for human rights and the rule of law – legality, legitimacy, legal certainty, proportionality, due process and fair trial. In the case concerning posting the harmful content the platform operator in fact needs to: 1) act legally, i.e., to make sure that the ToS (i.e. the contract with the user) provides the one with the opportunity to remove the content or to apply other sanction in this particular case; 2) find out whether the one's restrictive decision will have a justified aim (legitimacy) and will be adequate to this aim (proportionality); 3) ensure that the user will have an opportunity to lodge the one's complaint and to have it heard fairly, within a justified period of time and with due guarantees of impartiality (due process and fair trial).

Therefore, European fundamental values potentially may be applied horizontally, in particular, to cases stemming from modern contractual relationships inter alia arising on various online platforms. However, the role of values in this regard shall not be overestimated. What is crucial about values is not only that they outline the most progressive legal concepts, but that they are shared in the EU and

its Member States, which is only a part of the globe. As the latest decade shows there is a significant gap between values shared in the EU and in other parts of the world, in particular, in the autocratic jurisdictions (Russia, China, Iran, etc.), and this gap is constantly growing[81]. What we are observing during this decade is that what is valuable in the EU is not valuable in autocratic jurisdictions or at least the meaning of values is to a high extent distorted. Even the value system in the EU and in the USA has some differences, which is attested by various research papers[82]. Thus, considering the fact that most of the modern online platforms are incorporated outside the EU (mostly in the USA, but some of them – in the United Arab Emirates, Russia, China, etc.), one should not expect that they will share European fundamental values and seek to apply them in their contractual practice. What differs values from the concept of legal principles and human rights is that there is a world-wide consensus to share the latter, which is attested juridically, i.e. by way of ratifying or recognizing international legal documents concerning human rights (e.g. the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights etc.). Meanwhile, values are specific for particular communities and states, rarely – by the unions of the states (as the EU).

That is why the scope of horizontal effect of values will always be territorially and jurisdictionally limited, unless the common consensus on values is reached globally and current battles on this issue are minimized.

5. Conclusion

Contract law and contracting practice has changed significantly in the Digital Era. Micro-changes in contracting practice caused

[81] E. Engle, *A New Cold War? Cold Peace. Russia, Ukraine, and NATO,* in Saint Louis University Law Journal, Vol. 59, 2015, p. 99.

[82] M. Garlicki, *The Differences between American and European Approaches to Security Policy after the Cold War*, in *Przegląd Europejski*, Vol. 32/2, 2014, p. 70–80.

by technological development (electronic contracting, automatic and autonomous contract performance, etc.) have led to macro-changes of the whole concept of the contract. Contracts are no longer purely private instruments having a very limited scope of application – they are one of the most powerful instruments of regulation of relationships between Internet users, while their terms are turning into the rules touching upon fundamental human rights. Especially this is true for online platforms and contracts they conclude with their users: although these contracts involve only the relationships between a platform and its particular user, since there may be billions of users and all the contracts with them are the same, in the end the contracts become very powerful regulators.

Naturally, in modern academic discussions the issue of human rights protection by private entities (not only by states) has become more and more widespread and persuasive. Various concepts which traditionally have been attributed to the state and its area of responsibility are now regarded as concepts applicable to private relationships as well. This is especially true about human rights: although initially obligations concerning their protection were imposed on the states, today the possibility of horizontal effect of human rights is actively discussed. Obligations in the field of human rights are now attributed to businesses, especially to those who communicate and deal with the large number of consumers, in particular, to online platforms.

In this context a new question arises: may fundamental values outlined in the EU primary legislation be applied horizontally as well, in particular, to contractual relationships? Most of these values are based on human rights (right to life, freedom of association, right to found a family etc.) or human rights standards and guarantees (like democracy and the rule of law), and thus they are obviously interconnected with human rights. However,

the concept of fundamental values does not come down merely to human rights and their guaranties. First, values are broader categories than the categories of certain human rights. Second, values do not come down merely to legal concepts – they have a broader meaning which involves not only legal, but also cultural and philosophical categories. Third, the role of values differs from human rights: while the latter outline the measure of the permissible behavior and of the permissible interference with the area of personal freedom, the former outline what is valuable and what shall be guaranteed and defended.

However, these differences do not themselves mean that fundamental values cannot have a horizontal effect and may not be applied to private relationships, in particular, to contractual ones. Values can help courts, arbiters, and private parties evaluate acts, decisions or circumstances which arise in the modern contracting practice, i.e. to decide whether an act or a decision is based on the respect for human dignity and human rights, equality, solidarity, freedom, and the rule of law. Traditionally, in contractual relationships these are contract terms which are used as instructions of how to act and what to decide in relationships with the counterparty. However, in the Digital Era contract terms cannot always be sufficient, precise and reliable. Thus, fundamental values and human rights standards when applied horizontally may provide various entities and contracting parties with the needed instructions helping to make a balanced decision.

Meanwhile, the role of European fundamental values shall not be overestimated. These values are shared in the EU, but not across the whole globe. Thus, one should not expect that a platform operator incorporated in China or the USA will use the EU value system in the one's practice. In this regard the perspective of applying human rights standards horizontally looks more persuasive.

Preserving Privacy: Exploring Digital Silence in the European Context

Oksana Kiriiak*

Abstract: In the contemporary digital era, the notion of "digital silence" has emerged as a critical concept in discussions surrounding privacy, data protection, and online autonomy, particularly within the European Union (EU). This paper presents an in-depth analysis of the multifaceted phenomenon of digital silence, examining its definition, manifestations, legal implications, societal dynamics, and ethical considerations. Drawing upon extensive literature, case law, regulatory frameworks, and empirical research, this comprehensive study offers a nuanced understanding of digital silence and its significance in shaping the evolving landscape of digital rights and responsibilities in Europe. By exploring the intersections of law, society, and technology, this paper contributes to ongoing debates on digital privacy, data protection, and the ethical dimensions of digital behavior, offering insights for policymakers, legal scholars, technologists, and individuals navigating the complexities of the digital age.

Keywords: human rights; digital silence; right to privacy; right to be forgotten; right to erasure; digital freedom

1. Introduction

The evolution of human rights and freedoms stands as a pivotal achievement in the historical trajectory of societal legal development, tracing its origins from antiquity to the contemporary era, wherein human rights have evolved into an indispensable facet of democratic governance under the rule of law. As society progresses and cutting-edge digital technologies permeate our

* *PhD (Law), Associate Professor at the Private Law Department, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. E-mail: o.kiriyak@chnu.edu.ua*

existence, novel rights and modalities of their enforcement emerge, surpassing the imagination of earlier epochs. The proliferation of digital interaction platforms within mass culture reflects this unprecedented development, accompanied by a concomitant surge in legal complexities arising from the expansive reach and transformative potential of modern technologies. Moreover, the advent of legal constraints and regulations governing information dissemination underscores the evolving paradigm of state sovereignty, extending its purview to encompass the digital realm. In light of these multifaceted dynamics, contemporary legal discourse grapples with an array of emergent issues, necessitating nuanced legal analysis and adaptive regulatory frameworks to address evolving societal needs and safeguard fundamental rights in the digital age.

The advent of digital technology has revolutionized the way individuals interact, communicate, and navigate the world around them. However, alongside the benefits of digital connectivity, concerns about privacy, data protection, and online surveillance have become increasingly salient, prompting discussions about the concept of "digital silence" – the deliberate or involuntary absence or suppression of digital traces or data related to an individual's online activities. In the European context, where data protection regulations are among the most stringent globally, digital silence has emerged as a focal point in debates surrounding digital rights, freedoms, and ethical considerations. This paper seeks to explore the multifaceted nature of digital silence, examining its legal foundations, societal implications, and ethical dimensions within the European Union.

2. Exploring the notion of digital silence

Digital silence encompasses a diverse array of behaviors, practices, and circumstances that result in the absence or

suppression of digital data pertaining to an individual's online presence or activities. This may include strategies such as refraining from using digital devices or online platforms, employing privacy-enhancing technologies such as virtual private networks (VPNs) or encryption, or intentionally limiting the disclosure of personal information online. Digital silence can manifest in both voluntary and involuntary forms, reflecting individual choices, technological constraints, legal requirements, or social norms. While the concept of digital silence remains fluid and context-dependent, its implications for privacy, autonomy, and societal norms are profound, necessitating a nuanced examination of its legal and ethical dimensions.

2. 1. Legal framework

Within the European Union, the legal framework governing digital silence is anchored in the General Data Protection Regulation (GDPR), a comprehensive regulatory regime designed to safeguard individuals' rights to privacy and data protection. The GDPR affords individuals certain rights, including the right to erasure (commonly known as the "right to be forgotten"), which enables individuals to request the deletion or removal of their personal data from online platforms under specific circumstances. While the GDPR represents a significant milestone in data protection law, its application in practice raises complex legal and ethical questions regarding the balance between individual rights, freedom of expression, and public interests. Furthermore, the extraterritorial reach of the GDPR poses challenges for enforcing data protection standards across borders, particularly in an increasingly globalized and interconnected digital environment.

The European Union and the United States engage with the 3SI in recognition of the vital importance that greater economic convergence and a stable, interconnected, and economically

vibrant Central and Eastern Europe has for European stability and cohesion in an increasingly challenging geopolitical context, according to Frances G. Burwell F. G., Fleck J. (2020).[1]

European legislation addresses the concept of digital silence primarily through data protection regulations, with the General Data Protection Regulation (GDPR) serving as the cornerstone of legal frameworks across European Union (EU) member states. The GDPR grants individuals certain rights regarding the processing of their personal data, including the right to erasure, commonly known as the "right to be forgotten". This right allows individuals to request the deletion or removal of their personal data from online platforms under specific circumstances.

Various EU member states have implemented the GDPR into their national legislation, thereby providing legal mechanisms for individuals to exercise their rights related to digital silence. For example:

In France, the GDPR is complemented by the French Data Protection Act (Loi Informatique et Libertés), which regulates the processing of personal data and the exercise of data subjects' rights. The challenge of digital technology – as it was pointed out by Anaïs Theviot (2019)[2] is deeply societal: understanding computer thinking will be essential to not be left behind in a society where connected objects and algorithms will take a considerable place in the years to come. French courts have adjudicated cases involving the right to be forgotten, such as the landmark "Google Spain" case, where the Court of Justice of the European Union (CJEU) ruled that individuals have the right to request the removal of search engine links containing personal information that is inadequate, irrelevant, or no longer relevant.

[1] Frances G. Burwell F. G., Fleck J. The Next Phase of Digitalization in Central and Eastern Europe: 2020 and Beyond. Feb. 1, 2020. P. 8.

[2] Anaïs Theviot. Digitalization and Political Science in France. *Political Science and Digitalization – Global Perspectives*, 2019, p. 143.

Germany has enacted the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) to supplement the GDPR and address specific national requirements. Despite the phenomenon that the comparatively affluent country of Germany was always relatively late when it came to digital innovation, globalization enforced most of the trends, which Germany in time also implemented, since Norbert Kersting put it this way (2019).[3] German courts have interpreted and applied the GDPR in cases concerning the right to be forgotten, considering factors such as the balance between privacy rights and freedom of expression.

While no longer an EU member state, the UK has incorporated the GDPR into its national law through the Data Protection Act 2018. UK courts, including the Supreme Court and the Court of Appeal, have dealt with cases related to the right to be forgotten, providing guidance on its interpretation and application within the UK legal context.

These examples demonstrate how European legislation, including the GDPR and national data protection laws, addresses the concept of digital silence by providing individuals with legal mechanisms to control their personal data and exercise their privacy rights online. Through legislative frameworks and judicial decisions, European countries seek to strike a balance between protecting individuals' privacy and upholding other fundamental rights and societal interests.

Beyond its legal dimensions, digital silence has far-reaching societal implications, influencing patterns of online behavior, social interactions, and cultural norms within European societies. The phenomenon of digital silence reflects broader societal concerns about privacy, surveillance, and the erosion of personal autonomy in the digital age. Moreover, digital silence intersects with issues of digital exclusion, inequality, and discrimination, as individuals

[3] Norbert Kersting. Digitalization and Political Science in Germany. Political Science and Digitalization – Global Perspectives, 2019, p. 146.

from marginalized or vulnerable communities may face barriers to accessing or controlling their digital footprint. Understanding the societal dynamics of digital silence is crucial for informing policy debates, promoting digital literacy, and fostering inclusive and ethical practices in the digital realm.

In addition to its legal and societal dimensions, digital silence raises important ethical questions about the balance between individual privacy rights, freedom of expression, and the public interest. Ethical considerations surrounding digital silence encompass issues such as consent, transparency, accountability, and the ethical use of technology. As digital technologies continue to evolve and permeate all aspects of society, ethical frameworks and guidelines are needed to ensure that the benefits of digital innovation are balanced with the protection of individual rights and freedoms. Moreover, ethical debates surrounding digital silence extend beyond legal compliance to encompass broader questions about social responsibility, ethical leadership, and the ethical design and deployment of digital technologies.

The correlation between the right to be forgotten and the right to digital silence lies in their shared objective of empowering individuals to control their digital footprint and protect their privacy in the digital age. While the right to be forgotten focuses on the removal or delisting of specific personal information from online platforms, the right to digital silence encompasses a broader notion of managing one's online presence and minimizing digital traces altogether.

Both rights recognize the importance of individuals' autonomy over their personal data and seek to address the challenges posed by the permanence and ubiquity of information on the internet. By exercising the right to be forgotten, individuals can request the removal of outdated, inaccurate, or irrelevant information that may adversely affect their reputation or privacy. Similarly, the right to digital silence allows individuals to proactively control

the dissemination of their personal data and limit the exposure of sensitive information online.

Furthermore, the right to be forgotten and the right to digital silence are interconnected in their legal and technological implications. Legal frameworks such as the EU General Data Protection Regulation (GDPR) provide a legal basis for individuals to assert their rights to data privacy and protection, including the right to request the erasure of personal data (right to be forgotten). At the same time, advances in technology, such as privacy-enhancing tools and encryption methods, enable individuals to exercise greater control over their digital presence and maintain digital silence.

In practice, individuals may invoke both rights in tandem to achieve their privacy objectives. For example, someone seeking to minimize their digital footprint may use the right to be forgotten to remove specific instances of personal information from search results or social media platforms while also adopting privacy-enhancing measures to prevent the collection and dissemination of additional data. Conversely, exercising the right to digital silence by limiting online activities and data sharing may complement efforts to assert the right to be forgotten by reducing the amount of personal information available for indexing and dissemination.

Overall, the correlation between the right to be forgotten and the right to digital silence underscores the evolving nature of privacy rights in the digital era and the need for comprehensive legal and technological solutions to protect individuals' privacy and autonomy online.

2.2. Unraveling the right to be forgotten

Arguably, Vladimir Jankélévitch (2005)[4] posits that while it may be conceivable to navigate life without actively remembering, the act of forgetting is an inevitable facet of human existence:

[4] Jankélévitch, Vladimir. Forgiveness, *University of Chicago Press*, (2005), 27.

the ability to recollect the past enables societies to reconcile with historical events and move forward. This sentiment resonates with the assertions of Viktor Mayer-Schönberger (2011),[5] who contends that in an era where remembrance has become ubiquitous, there arises a parallel imperative for the right to be forgotten. As Chanhee Kwak et al. (2021)[6] underscore, the advent of information and communication technologies has ushered in a paradigm shift in human memory, exponentially augmenting its storage and retrieval capacities. The proliferation of digital records has rendered moments of individuals' lives indelible, transforming the perception of memory from ephemeral to enduring. Consequently, this evolution raises profound questions regarding the implications of digital memory on personal autonomy, privacy rights, and societal norms surrounding forgiveness and reconciliation. In navigating this terrain, legal scholars and policymakers must grapple with the intricate balance between the preservation of historical truth, the protection of individual privacy, and the promotion of societal healing and progress.

This discovery lends credence to Cayce Myers' assertions (2014)[7] regarding the contemporary challenge posed by the digitalization of personal history. Unlike previous epochs, where an individual's past was preserved through tangible artifacts like photographs, diaries, and collective memories, the digital age confers a form of immortality through online presence. Delving into

[5] Mayer-Schönberger, Viktor. (2011). Delete: The virtue of forgetting in the digital age. Princeton: *Princeton University Press*. (2011), 165.

[6] Kwak Chanhee, Lee Junyeong, Lee Heeseok. Could You Ever Forget Me? Why People Want to be Forgotten Online. (2021) *Journal of Business Ethics*. https://www.scopus.com/record/display.uri?eid=2-s2.085100146466&origin=resultslist&sort=plf-f&src=s&st1=&st2=&sid=0daeb36f35186b6eecf36fa91bb91586&sot=b&sdt=b&sl=36&s=TITLE-ABS-KEY%28right+to+be+forgotten%29&relpos=3&citeCnt=0&searchTerm=

[7] Myers, Cayce. Digital Immortality vs. "The Right to be Forgotten": A Comparison of U. S. and E. U. Laws Concerning Social Media Privacy. *Revista Română de Comunicare şi Relaţii Publice*. No: 3XVI. (2014), 48.

the scholarly discourse on this subject, Meg Leta Jones (2018)[8] highlights the internet's transformation into a vast repository of searchable data, serving as a dynamic cultural memory with multifaceted implications. This narrative aligns with Viktor Mayer-Schönberger's (2011)[9] findings, which underscore the irreversible entwinement of personal actions with digital footprints, rendering escape from one's past a practical impossibility. Consequently, this phenomenon engenders a host of legal and ethical considerations pertaining to privacy, data protection, and individual autonomy. As society grapples with the ramifications of ubiquitous digital memory, legal scholars are tasked with navigating the complexities of balancing historical preservation, personal privacy, and the right to be forgotten in the digital age.

The innate desire for individuals to control certain aspects of their personal information within the public domain is inherently reasonable and often universally recognized. However, translating this desire into actionable legal mechanisms within societies that champion openness and freedom of expression presents considerable challenges. As Rebekah Larsen (2020)[10] aptly observes, the right to be forgotten (RTBF) is not an absolute entitlement under the law; rather, it must be judiciously balanced against competing fundamental rights, particularly the right to freedom of expression, which serves as a cornerstone of democratic societies. This nuanced interplay between individual privacy rights and broader societal interests underscores the complex nature of legal and ethical considerations surrounding the implementation of RTBF regulations. Moreover, the evolution of digital technologies

[8] Jones, Meg Leta. Ctrl + Z: The Right to Be Forgotten. *NYU Press* (2018), 5.

[9] Mayer-Schönberger, Viktor. Delete: The virtue of forgetting in the digital age. Princeton: *Princeton University Press*. (2011), 163–164.

[10] Larsen, Rebekah. Mapping Right to be Forgotten frames: Reflexivity and empirical payoffs at the intersection of network discourse and mixed network methods. *New media & society*. Vol. 22(7), (2020), 1246.

and the exponential growth of online content further complicate matters, necessitating ongoing deliberation and refinement of legal frameworks to effectively address contemporary challenges. In navigating this intricate landscape, legal scholars and policymakers must strive to strike a delicate balance that upholds individual autonomy while safeguarding the collective interests of society. This requires a nuanced understanding of the evolving dynamics between privacy, freedom of expression, and the public interest, coupled with a commitment to fostering a legal environment that promotes accountability, transparency, and respect for human rights in the digital age.

In the contemporary legal landscape, there is a growing recognition of the imperative to reconcile human rights principles with positive law, viewing them not as mutually exclusive entities but rather as integral components of a cohesive legal framework. It is increasingly evident that a nuanced and modern normative legal perspective is essential for addressing the inherent tensions between traditional legal norms and evolving human rights standards, thereby fostering a more harmonious integration of these elements within legal practice. This necessitates a paradigm shift in the perception of human rights from mere ideological constructs to tangible legal realities, thereby enabling law enforcement agencies to navigate the complexities of human rights law with greater efficacy and precision. Central to this discourse is the notion of human rights as a dynamic legal construct, demanding rigorous interpretation and application to ensure optimal outcomes in law enforcement and judicial decision-making.

An ideal litmus test for exploring the intersection between human rights and digital memory lies in the realm of the right to be forgotten (RTBF), a concept that has yet to be fully integrated into the Ukrainian legal framework. As such, the RTBF serves as a compelling case study for examining the progressive evolution

of legal perceptions and interpretative methodologies in response to emerging legal phenomena. The nascent status of the RTBF within the Ukrainian legal system offers a unique opportunity to scrutinize its reception and implementation through the lens of positive legal norms, interpretive frameworks, and evolving jurisprudential approaches. By engaging with the RTBF in this context, legal scholars and practitioners can gain valuable insights into the broader dynamics of human rights law in the digital age, thereby contributing to the ongoing refinement of legal theory and practice in Ukraine and beyond.

The pluralism of approaches to the RTBF reflects the interdisciplinary nature of contemporary legal scholarship, drawing upon insights from various fields such as law, ethics, sociology, and information science to elucidate its legal and societal implications. Scholars have explored a range of conceptual frameworks and methodological approaches to understand the complexities of the RTBF, enriching the scholarly discourse and advancing nuanced understandings of its normative dimensions. Moreover, the plurality of perspectives underscores the inherent tensions between competing rights and interests, including privacy, freedom of expression, and access to information, in the digital realm. Rebekah Larsen's contributions (2020)[11] to this discourse is notable, particularly her insights into the pluralistic and democratic ethos of information networks, which serve as platforms for the exchange of diverse perspectives and methodologies in legal scholarship. By engaging with this diversity of viewpoints, scholars can deepen their understanding of the ethical and legal complexities inherent in the RTBF and contribute to the development of more robust and contextually relevant legal frameworks.

In the contemporary landscape of legislative practice, a plethora of approaches emerge when dissecting the pertinent question

[11] Larsen, Rebekah. *New media & society*, 1247.

at hand. These diverse perspectives offer valuable insights into the multifaceted nature of legal discourse and underscore the complexity inherent in defining the subject matter.

Firstly, it is imperative to explore the conceptual nuances surrounding the topic, delving into the various interpretations offered by legal scholars and practitioners alike. This entails scrutinizing the definitional parameters from multiple angles to gain a comprehensive understanding of the subject's scope and implications. Secondly, contextual factors must be taken into account, as the interpretation of legal concepts often hinges on the specific legal, cultural, and societal contexts in which they are applied.

Furthermore, historical perspectives shed light on the evolution of legal definitions over time, highlighting shifts in societal norms, technological advancements, and jurisprudential paradigms. By tracing the trajectory of definitional frameworks, we can discern patterns of continuity and change, illuminating the underlying principles that inform contemporary legal discourse. Additionally, comparative analysis offers valuable insights by juxtaposing divergent approaches across different jurisdictions and legal systems.

Moreover, interdisciplinary perspectives enrich the discourse by drawing upon insights from adjacent fields such as philosophy, sociology, and linguistics. These interdisciplinary exchanges foster a more holistic understanding of the subject matter, transcending traditional disciplinary boundaries and enhancing the richness of legal scholarship. Ultimately, by engaging with a diverse array of definitional frameworks and methodological approaches, we can navigate the complexities of the subject with greater nuance and depth, contributing to the advancement of legal theory and practice.

In our assessment, several definitional frameworks warrant consideration as we navigate the intricacies of this issue: (1) a right

to removal (Selen Uncular, 2019),[12] (2) a right to suppression (Christopher Kuner, 2015),[13] (3) a right of oblivion (Cayce Myers, 2014).[14]

Considering the elucidation provided by the aforementioned definitions, it is our contention that there exists no basis for antagonism among them; rather, they are poised to complement one another, fostering a multifaceted examination of the subject matter. This harmonious coexistence of diverse viewpoints enables a comprehensive exploration of the intricacies inherent in the topic, affording the opportunity to leverage varied perspectives in probing the same issue from different angles.[15] Moreover, advocates for the expanded utilization of this legal construct converge in their recognition of the right to be forgotten (RTBF) as an avenue for individuals to unburden themselves from past encumbrances and embark on a fresh start unencumbered by historical baggage.

Conversely, neglecting any of the constituent elements delineated above jeopardizes the integrity of the overarching framework governing the RTBF, thus undermining the holistic understanding of this legal prerogative. As underscored by Mattias Goldmann (2020),[16] the RTBF holds relevance across multiple

[12] Uncular, Selen. The right to removal in the time of post-Google Spain: myth or reality under general data protection regulation?, *International Review of Law, Computers & Technology*, Vol. 33 /3 (2019), 310.

[13] Kuner, Christopher. The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines, LSE Law, Society and Economy Working Papers 3/2015, p. 7, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496060 (last accessed 14.02.2020).

[14] Myers, Cayce. Digital Immortality vs. "The Right to be Forgotten": A Comparison of U. S. and E. U. Laws Concerning Social Media Privacy. *Revista Română de Comunicare şi Relaţii Publice*. No: 3XVI. (2014), 48.

[15] Pagallo, Ugo and Durante, Massimo. Legal Memories and the Right to be Forgotten, in L. Floridi (eds.), Protection of Information and the Right to Privacy – A New Equilibrium? *Springer Verlag*, (2014), 19.

[16] Goldmann, Mattias. As Darkness Deepens: The Right to be Forgotten in the Context of Authoritarian Constitutionalism. *German Law Journal*. 21. (2020), 53.

domains, and it is only through a comprehensive consideration of its manifold dimensions that its true significance emerges. By embracing the multiplicity of perspectives and acknowledging the interconnectedness of its various facets, the concept of the RTBF emerges as a nuanced and indispensable component of contemporary legal discourse.

Significantly, within the legal framework, the right to be forgotten (RTBF) is not construed as an absolute entitlement; rather, it necessitates a delicate equilibrium with "other fundamental rights", as per recognized legal precepts.[17] The notion of curtailing rights and freedoms is presently enshrined as a normative principle under international law, as elucidated by Robert Tabaszewski (2020).[18] Furthermore, the interconnection between the observance of human rights and business ethics, particularly within the realm of corporate social responsibility, has garnered increasing attention in contemporary discourse. This paradigm shift reflects a departure from the laissez-faire ethos of unbridled capitalism towards a more socially conscious approach to entrepreneurship, as highlighted by Kinga Machowicz (2021).[19]

Nevertheless, the expanding ambit of EU data protection law, inclusive of the right to be forgotten, has encountered mounting challenges regarding jurisdictional boundaries, as noted by Federico Fabbrini and Edoardo Celeste (2020).[20] This ongoing

[17] Larsen, Rebekah. Mapping Right to be Forgotten frames: Reflexivity and empirical payoffs at the intersection of network discourse and mixed network methods. *New media & society*. Vol. 22(7), (2020), 1246.

[18] Tabaszewski, Robert. The Permissibility of Limiting Rights and Freedoms in the European and National Legal System due to the Health Protection. *Review of European and Comparative Law*. Vol. XLII, Issue 3, (2020), 54.

[19] Machowicz, Kinga. Observance of human rights as an element of shaping the position of the European enterprise in the knowledge-based economy. *Review of European and Comparative Law*. Issue 1, (2021), 16.

[20] Fabbrini, Federico and Celeste, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal* 21, (2020), 56.

debate underscores the need for a nuanced understanding of the interplay between legal principles and technological advancements in the digital age. As the landscape of data privacy continues to evolve, legal scholars and practitioners alike are tasked with navigating the complex terrain of jurisdictional sovereignty and transnational cooperation in safeguarding individual rights within an increasingly interconnected global context.

As underscored by Jennifer Daskal (2018),[21] an escalating number of judicial proceedings worldwide have brought forth "critically important questions about the appropriate scope of global injunctions, the future of free speech on the internet, and the prospect for harmonization (or not) of rules regulating online content across borders". These assertions carry significant weight, considering that until recently, domestic jurisprudence largely confined discussions on forgetting within the purview of mundane human oversight or grammatical errors. Instances of forgetfulness cited in judicial texts often pertained to trivial matters such as forgetting one's name, failing to affix a seal, or overlooking a promissory note, among others. Even colloquial references, like the village of Zabuttya (Oblivion) in the Khmelnytsky region of Ukraine, were invoked within this narrow context.

However, beneath the surface lies a broader, global predicament, as astutely articulated by Mattias Goldmann (2020),[22] who posits that the cases adjudicated by the Court of Justice of the European Union (CJEU) in recent years merely scratch the surface of a much larger issue. These legal deliberations represent only a fraction of the myriad complexities surrounding the right to be forgotten and its implications for individual privacy, freedom of expression, and

[21] Daskal, Jennifer. Google, Inc v. Equustek Solutions. *American Journal of International Law,* Volume 112, Issue 4, (2018), 730.

[22] Goldmann, Mattias. As Darkness Deepens: The Right to be Forgotten in the Context of Authoritarian Constitutionalism. *German Law Journal*. 21. (2020), 46.

transnational legal frameworks. As legal scholars and practitioners grapple with these multifaceted challenges, it becomes imperative to foster interdisciplinary dialogue and collaborative efforts aimed at navigating the evolving landscape of digital rights and responsibilities in the 21st century.

Rather than confining the usage of the term "RTBF" solely within the domain of comparative law and scholarly discourse, recent developments warrant its application in a more concrete, literal sense as delineated in EU Directives. For instance, in a notable case brought before the Desniansky District Court of Chernihiv in May 2018 (case № 750/5021/18, proceedings № 4-s/750/45/18[23]), PERSON_1 filed a complaint against the actions and inaction of the chief state executor of the Central Department of the State Executive Service of Chernihiv city, within the Main Territorial Department of Justice in the Chernihiv region. In their complaint, PERSON_1 specifically invoked the provisions of "RTBF", as outlined in Article 17 of the General Data Protection Regulation of the European Union. This legal recourse underscores a paradigm shift towards the direct invocation of EU regulations within Ukrainian legal proceedings, marking a significant departure from traditional jurisprudential practices.

However, this isolated instance represents merely a fraction of the potential scope of judicial challenges pertaining to the implementation of RTBF within Ukrainian legal frameworks. As stakeholders continue to grapple with the intricacies of data protection and privacy rights in an increasingly digitized world, achieving consensus on the application and interpretation of RTBF remains an ongoing challenge. Moreover, the convergence of legal norms and practices across diverse jurisdictions underscores the need for harmonization and standardization efforts to ensure

[23] Desniansky District Court of Chernihiv. Juidgement of 25 May 2018 https://reyestr.court.gov.ua/Review/74269229 (accessed on 31.03.2021).

consistent and equitable treatment of individuals' rights across borders. As such, ongoing dialogue and collaboration among legal scholars, policymakers, and practitioners are essential to navigate the evolving landscape of data privacy and protection in the digital age.

The divergence in scholarly interpretations regarding the essence of RTBF serves as a counterbalance to the prevailing consensus among state authorities, who often adhere to antiquated standards in evaluating social phenomena, particularly within the digital realm. In parallel, the framework of post-Soviet legal reasoning and jurisprudence does not consistently accommodate the nuances of Ukrainian legal culture and the distinctive characteristics of the country's academic landscape. In this context, the scholarly insights articulated by Jure Globocnik (2020)[24] merit consideration, as they underscore the complexity of delineating boundaries in the online sphere and highlight the far-reaching implications of judicial decisions, not only for internet users but also for technology companies operating within and beyond the EU. Moreover, Globocnik's observations shed light on the pioneering role of the Court in shaping the discourse on the right to be forgotten, suggesting that its rulings may indirectly influence legislative frameworks and judicial precedents in non-EU jurisdictions. Consequently, these multifaceted dynamics underscore the need for a nuanced and contextually informed approach to legal scholarship and policy-making in the digital age, one that acknowledges the interconnectedness of legal regimes and the transnational nature of contemporary legal challenges.

However, the most glaring legal inconsistency arises not merely from a court's denial of a petitioner's RTBF claim, but

[24] Globocnik, Jure. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17), *GRUR International*, 69(4), (2020), 388.

rather from a decision that affirms such a claim. In such instances, the judgment typically contains comprehensive information about the case's parties and particulars, which, once made public, may subsequently be targeted for removal by one of the involved parties. Paradoxically, even if redacted, these details remain accessible to an indeterminate audience through online repositories of judicial records. These texts serve as integral components of legal education at various academic levels, forming the basis for scholarly dissertations and continuing to inform judicial deliberations across jurisdictions. Moreover, they often feature in public discourse, disseminated through newspapers and periodicals, and subject to analysis and debate by diverse segments of society over an extended period. This underscores the intricate interplay between legal proceedings and broader societal dynamics, necessitating careful consideration of the implications of RTBF rulings on the dissemination of legal information and the functioning of democratic institutions.

Invariably, the outcome is antithetical to the intended objective – wherein information, the deletion of which from the online domain constituted the primary aim of the petitioner's legal action, persists in proliferating across digital platforms, perpetuating its accessibility for an indeterminate span of time to an extensive audience. Despite potential amendments to regulatory texts and the explicit stipulation mandating closed-court deliberations for cases of this nature, ensuring confidentiality, the practical efficacy of such measures remains questionable. This underscores the inherent challenges in effectively enforcing the right to be forgotten, particularly in jurisdictions beyond the purview of the European Union (EU), where such data remains accessible through the original source's web portal. Moreover, the circumvention of geographical restrictions via virtual private networks (VPNs) or similar technological tools further complicates

the enforcement of data removal mandates, underscoring the intricate interplay between legal principles and technological capabilities in contemporary jurisprudence.

A consistent paradox pervades all instances within this category, a phenomenon underscored notably by Jure Globocnik (2020),[25] who cogently articulates the nuances: "Referred to commonly as the right to de-referencing, this pertains to a data subject's ability to petition a search engine operator to eliminate (de-reference) links from search results leading to websites containing personal data pertinent to them, particularly if such data are deemed inadequate, irrelevant, or obsolete in relation to their original purposes of collection and processing. It warrants emphasis that this prerogative is contingent upon searches conducted using the data subject's name; links may still manifest in search results when employing alternative search terms. Additionally, the visibility of a link in search results must be distinguished from the initial publication of information, obligating the data subject to exercise their right to be forgotten independently with regard to each. Moreover, notwithstanding the de-referencing of information from search results, its presence on the webpage of initial publication persists, unless the data subject successfully asserts their right to erasure vis-à-vis the web page publisher as well".

Expanding upon this observation, it is imperative to scrutinize the multifaceted ramifications of the right to de-referencing within the broader framework of data protection law. Globocnik's elucidation underscores the intricate balance between an individual's right to privacy and the public's right to access information. Moreover, the delineation of specific criteria for the exercise of this right, such as the inadequacy or irrelevance of data,

[25] Globocnik, Jure. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17), *GRUR International*, 69(4), (2020), 380.

introduces additional layers of complexity in its interpretation and application. Furthermore, the practical implications of this right extend beyond mere removal from search results, necessitating considerations regarding the enduring visibility of information on the original webpage and the potential recourse available to data subjects in compelling its deletion. This intricate interplay between legal principles and technological mechanisms underscores the evolving nature of data protection jurisprudence in the digital age, prompting ongoing scholarly discourse and legislative scrutiny.

A minor, albeit equally consequential, augmentation to the aforementioned considerations, from our vantage point, necessitates a recalibration of the procedural regulations governing trials within this particular domain. As the arbiter of a diverse array of disputes, the Judge grapples with the task of harmonizing the interests of the litigants, who contest against excessive public exposure of their grievances, and those of the society, which endeavors to uphold the impartiality of the judiciary. Addressing this predicament may hinge upon implementing measures to broaden the scope of closed-court proceedings and corresponding confidential adjudications across all legal proceedings entailing the execution of the Personal Rights Regime (PRR), encompassing both digital and traditional paper-based formats. Consequently, while the removal of information from the internet would indeed curtail access for residents within the European Union, its availability to individuals beyond these borders remains unaffected.

Expanding on this, the revision of procedural norms in trials concerning the enforcement of personal rights in the digital realm presents a multifaceted challenge. The judiciary finds itself at the nexus of conflicting interests, balancing the imperative of safeguarding privacy against the principle of open justice. In this context, enhancing the framework for closed-court sessions emerges as a potential solution, affording parties greater control

over the dissemination of sensitive information while preserving judicial transparency. Moreover, extending the applicability of confidential court decisions to all matters pertaining to the implementation of the PRR underscores a commitment to consistency and comprehensive protection of personal rights across legal proceedings.

Furthermore, the nuanced interplay between privacy rights and judicial transparency underscores the evolving landscape of digital jurisprudence. By exploring avenues to refine procedural rules, the legal system endeavors to adapt to the complexities of the digital age while upholding fundamental principles of fairness and accountability. However, it is imperative to recognize the global nature of information dissemination, wherein the removal of content from online platforms may not necessarily impede access outside the jurisdiction of the European Union. This underscores the intricate dynamics at play in reconciling competing interests within the realm of digital rights enforcement.

There exists a distinct cohort of scholars who adopt a cautious stance towards the ramifications brought forth by the Right to Be Forgotten (RTBF) within the established landscape of information utilization. While refraining from outright rejection of the applicability of this right, they exhibit a reserved demeanor towards its overarching legitimacy. This faction of researchers neither wholly advocates for nor refutes the fairness of its existence. One notable proponent of this viewpoint is David Erdos, whose scholarly inquiries, as evidenced in his statement from 2021, suggest a nuanced perspective. Erdos posits that data protection measures ought to facilitate individuals in exerting a certain degree of retrospective control over the dissemination of their online data, albeit with circumspection.[26]

[26] Erdos, David. The right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps. *Journal of Media Law.* (2021) *https://*

Originating from the European Union (EU), the RTBF serves as a quintessential exemplar of this paradigm shift. Enshrined within Article 17 of the General Data Protection Regulation (GDPR), the RTBF delineates the entitlement of individuals "to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay" (European Parliament, 2016, p. 43).[27] This legislative provision underscores the evolving landscape of data protection jurisprudence and underscores the imperative for balancing individual privacy rights with the exigencies of data processing and dissemination within the digital realm.

Moreover, Erdos' scholarly intervention prompts a critical reevaluation of the ethical, legal, and societal implications of the RTBF. By interrogating the tension between individual autonomy and collective information access, Erdos challenges conventional assumptions about the contours of data privacy and accountability in the digital age. His nuanced perspective highlights the need for a deliberative approach towards crafting legislative frameworks that reconcile competing interests and safeguard fundamental rights.

Furthermore, the inclusion of the RTBF within the GDPR signifies a paradigmatic shift in data protection governance, marking a departure from conventional regulatory approaches towards a more rights-based framework. This legislative milestone underscores the growing recognition of individuals' rights to control the dissemination and retention of their personal data, thereby empowering them to assert agency over their digital identities.

www.scopus.com/record/display.uri?eid=2-s2.0-85101100662&origin=resultslist&sort=plf-f&src=s&st1=&st2=&sid=0216523637ab63ccc03b179735abd04f&sot=b&sdt=b&sl=36&s=TITLE-ABS-KEY%28right+to+be+forgotten%29&relpos=2&citeCnt=0&searchTerm=

[27] European Parliament. (2016). 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. *Oficial Journal of the European Union* (OJ), 59(1–88), 294.

In conclusion, the cautious scholarly discourse surrounding the RTBF underscores the complexity of reconciling individual privacy rights with broader societal interests in information access and transparency. Erdos' nuanced perspective calls attention to the multifaceted nature of data protection challenges and underscores the imperative for a balanced and context-sensitive approach to regulatory intervention in the digital domain.

The territorial dimension of the Right to Be Forgotten (RTBF) warrants meticulous examination, given its current application limited to the jurisdiction of the European Union (EU), with the seminal ruling originating from the European Court of Justice in 2014. This assertion is predicated on the notion elucidated by Federico Fabbrini and Edoardo Celeste (2020),[28] positing the EU as a vanguard in global data protection endeavors. Consequently, as inferred from Meg Leta Jones' scholarly discourse (2018),[29] pivotal cases addressing multifaceted issues of reputation, identity, privacy, and memory in the Digital Age were adjudicated on the same day, yet yielded disparate outcomes on opposite sides of the Atlantic.

The first case, originating in Spain (Google Spain SL, Google Inc. v AEPD, Mario Costeja González), laid the cornerstone for the RTBF's application across the EU. Conversely, the second case, unfolding in the United States, involved American Idol contestants litigating against Viacom, MTV, and other defendants over online content resulting in their disqualification from the television show. While delving into the intricacies of litigation may seem tangential to our research, it is imperative to underscore that analogous scenarios elicited divergent judicial determinations in Europe and America.

[28] Fabbrini, Federico and Celeste, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal* 21, (2020): 55.

[29] Jones, Meg Leta. "Ctrl + Z: The Right to Be Forgotten." *NYU Press* (2018), 11–12.

Despite the historical significance of the court ruling in the first case, which paved the way for RTBF enforcement in the EU, the protracted appeals process in the second case engendered a nuanced juxtaposition of the judicial stances adopted. Indeed, a more antagonistic interpretation of these contrasting decisions may emerge. Thus, aligned with Fabbrini's assertions (2020),[30] contemporary society operates within a global digital milieu transcending national borders. Consequently, individuals' right to data protection may be compromised even when search engine results are displayed in a country divergent from the data subject's domicile.

Furthermore, the transnational ramifications of RTBF adjudication underscore the imperative for harmonizing legal standards and procedural mechanisms across jurisdictions. As digital interconnectedness proliferates, the need for cross-border cooperation and mutual recognition of privacy rights becomes increasingly salient. In this vein, ongoing scholarly inquiry and interdisciplinary dialogue are pivotal in navigating the complex terrain of digital jurisprudence and safeguarding individuals' rights in an interconnected world.

Upon juxtaposing the challenges delineated on a global scale, the Ukrainian scenario, characterized by its ineffectual legislation and unconditional litigation practices, appears rather commonplace. As articulated by Cayce Myers (2014),[31] disparities between the European Union and the United States regarding confidentiality exemplify the multifaceted obstacles engendered by these emerging directives. The ongoing struggle for privacy

[30] Fabbrini, Federico and Celeste, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal* 21, (2020), 64.

[31] Myers, Cayce. Digital Immortality vs. "The Right to be Forgotten": A Comparison of U. S. and E. U. Laws Concerning Social Media Privacy. *Revista Română de Comunicare şi Relaţii Publice*. No: 3XVI. (2014), 59.

rights and the Right to Be Forgotten (RTBF) underscores palpable tensions between individual rights and corporate interests, epitomizing the divergent trajectories of private law practice in the United States and Europe.

Simultaneously, the ubiquitous nature of the World Wide Web has fostered a heightened global discourse, accentuating legal and ideological disparities akin to tectonic shifts. This dichotomy between the ethos of free speech and self-expression and the imperative of legal regulation underscores the intricate dynamics at play in contemporary jurisprudence. Nonetheless, aligning with the perspective espoused by Mattias Goldmann (2020),[32] it is indisputable that RTBF rulings mark a seminal moment in the evolution of judicial discourse.

Indeed, the interplay between legal systems and cultural norms across continents underscores the imperative for nuanced approaches to privacy rights in an increasingly interconnected world. As legal frameworks continue to grapple with the complexities of digital jurisprudence, fostering cross-jurisdictional dialogue and harmonizing legal standards become imperatives in safeguarding individual rights and navigating the evolving landscape of global governance. Consequently, ongoing scholarly inquiry and interdisciplinary collaboration are pivotal in shaping the contours of digital rights and ensuring equitable access to justice in the digital age.

3. Anticipating future trends

In recent years, European trends in the development of the concept of digital silence have been shaped significantly by legislative efforts aimed at safeguarding individuals' privacy rights in the digital sphere. The General Data Protection Regulation (GDPR),

[32] Goldmann, Mattias. As Darkness Deepens: The Right to be Forgotten in the Context of Authoritarian Constitutionalism, *German Law Journal* 21. (2020), 46.

which came into effect in May 2018, stands as a pivotal piece of legislation influencing these trends. The GDPR grants individuals within the European Union (EU) a range of rights concerning the processing of their personal data, including the right to erasure, commonly known as the "right to be forgotten".

One prominent trend in the development of digital silence within the European context is the increasing recognition of individuals' rights to control their online presence and reputation. The right to be forgotten, enshrined in Article 17 of the GDPR, empowers individuals to request the deletion or removal of their personal data from online platforms under specific circumstances. This right reflects a broader societal shift towards recognizing the importance of privacy and data protection in the digital age.

Furthermore, European countries have seen a growing emphasis on accountability and transparency in data processing practices. Organizations subject to the GDPR are required to implement robust data protection measures, including mechanisms for obtaining consent, data minimization, and accountability. These requirements aim to enhance individuals' trust in the handling of their personal data and promote responsible data management practices among organizations.

Concurrently, a notable trend emerges wherein the significance of a timely and appropriate intervention by pertinent authorities to address issues arising from the utilization of the legal framework governing the Right to Be Forgotten (RTBF) in specific real-life scenarios and contentious legal contexts is being marginalized. Regrettably, the scholarly and theoretical assertions posited by detractors contesting the validity and subsequent practical enactment of the RTBF are wielded as a legal rationale for rejecting the pleas of plaintiffs, which squarely fall within the ambit of the legal provisions governing the application of the RTBF currently under scrutiny.

This phenomenon underscores the complex interplay between legal theory, practical application, and judicial decision-making within the realm of digital rights enforcement. As proponents of the RTBF advocate for its recognition and enforcement as a fundamental component of privacy protection in the digital age, detractors counter with arguments questioning its legitimacy and feasibility in practical application. Consequently, the response of relevant authorities to navigate these nuanced legal intricacies becomes paramount in ensuring equitable outcomes for all parties involved.

Moreover, delving deeper into the discourse surrounding the RTBF reveals a spectrum of divergent perspectives and interpretations among legal scholars and practitioners. While some advocate for a robust and expansive interpretation of the RTBF to afford individuals greater control over their digital footprint, others espouse a more circumspect approach, citing concerns regarding potential encroachments on freedom of expression and information dissemination. Thus, the resolution of disputes involving the RTBF necessitates a judicious balancing of competing rights and interests within the framework of established legal principles and precedents.

Furthermore, the evolving nature of digital rights jurisprudence underscores the need for ongoing dialogue and engagement among stakeholders to refine and adapt legal frameworks to the dynamic realities of the digital landscape. By fostering collaboration between legal scholars, practitioners, policymakers, and technology experts, it becomes possible to develop nuanced and effective strategies for navigating the complex intersection of law and technology. Ultimately, the adequacy of responses from relevant authorities in addressing issues pertaining to the RTBF will play a pivotal role in shaping the trajectory of digital rights enforcement and privacy protection in the digital era.

The lapse of time within the depicted scenarios has precipitated what has been aptly characterized by Jeffrey Rosen (2012)[33] as a regrettable misinterpretation; notably, the ruling in Google Spain did not establish a novel entitlement but rather elucidated the parameters of the right to erasure. Proponents aligned with this viewpoint contend that the actual implementation of a robust Right to Be Forgotten (RTBF) framework could potentially imperil the fundamental right to freedom of expression. This perspective is further expounded upon by Emily Adams Shoor (2014),[34] who argues that the adverse ramifications stemming from widespread adoption of the RTBF would outweigh its purported benefits. Furthermore, the German Association of Internet Economy contends that uniform standards should govern both online and offline publications, advocating for parity in regulatory treatment across digital and traditional media spheres.[35]

This discourse underscores the multifaceted nature of the ongoing debate surrounding the RTBF, which intersects complex legal, ethical, and societal considerations. Critics argue that the RTBF, if implemented without due consideration for its potential implications, could inadvertently stifle public discourse and impede the free flow of information essential to democratic societies. Conversely, proponents contend that the RTBF serves as a crucial mechanism for safeguarding individual privacy rights in an era characterized by ubiquitous digital surveillance and data collection.

Moreover, the nuanced legal and ethical considerations inherent in the RTBF debate necessitate a comprehensive examination

[33] Rosen, Jeffrey. The Right to Be Forgotten, *Stanford Law Review*, Symposium Issue, (2012), 88–95.

[34] Adams Shoor, Emily. Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation, *Brooklyn Journal of International Law*, 2014, Vol 39, (2014): 487–521.

[35] Bundesverfassungsgericht, Recht of freie Entfaltung der Persönlichkeit. 1 (BvR 16/13), 19.

of its potential ramifications across various jurisdictions and contexts. While proponents advocate for the adoption of robust data protection measures to empower individuals to assert control over their personal information online, detractors caution against overreaching regulatory interventions that could unduly restrict legitimate forms of expression and access to information.

Additionally, the evolving nature of digital rights jurisprudence underscores the need for ongoing dialogue and collaboration among stakeholders to develop balanced and effective regulatory frameworks. By fostering interdisciplinary engagement between legal experts, policymakers, technology professionals, and civil society representatives, it becomes possible to navigate the complex terrain of digital rights enforcement while upholding fundamental principles of democracy, transparency, and individual autonomy.

Furthermore, as the RTBF continues to garner attention on the global stage, there is a growing imperative to address emerging challenges and ambiguities surrounding its implementation. This includes clarifying the scope of the RTBF, establishing clear procedural guidelines for its application, and striking a delicate balance between privacy protection and freedom of expression in the digital realm. Ultimately, the effective resolution of these issues will require concerted efforts from all stakeholders to reconcile competing interests and uphold the principles of justice and equity in the digital age.

This rationale possesses inherent cogency for several discernible reasons. When considering the removal of information from digital platforms such as online periodicals, it is imperative to acknowledge that analogous information dissemination may occur through traditional print media, necessitating comprehensive coverage by any court-ordered action – an endeavor fraught with practical challenges. For instance, envisioning a scenario wherein

identical information is concurrently published in electronic and paper formats, perhaps within the pages of a single publication amalgamating online and offline publishing activities, legislative coherence in addressing this issue becomes paramount. Essentially, any directive aimed at expunging information from online search engine results must logically extend to the obliteration of the same data from the entire print circulation – an undertaking deemed impracticable due to logistical constraints. Indeed, the sheer passage of time renders it physically unfeasible to identify every holder of a specific newspaper or magazine edition, thereby underscoring the formidable obstacles associated with achieving comprehensive removal of printed content.

This line of reasoning underscores the intricate interplay between digital and traditional media landscapes, necessitating a nuanced approach to regulatory interventions aimed at safeguarding individual rights in the digital age. As technological advancements continue to reshape the media ecosystem, policymakers face the formidable task of reconciling competing imperatives while preserving fundamental principles of justice and equity. Moreover, the evolving nature of information dissemination underscores the need for adaptable legal frameworks capable of addressing emerging challenges in a holistic manner.

Furthermore, the jurisdictional complexities inherent in cross-border data flows and digital content dissemination further compound the challenges associated with regulating information removal requests. In an interconnected global landscape, the reach of digital content transcends national boundaries, necessitating harmonized approaches to data protection and privacy regulation. However, achieving consensus on regulatory standards and enforcement mechanisms remains a formidable task, given the divergent legal traditions and cultural norms prevalent across jurisdictions.

Moreover, the proliferation of digital platforms and the democratization of content creation have democratized access to information while simultaneously exacerbating concerns related to data privacy and security. As individuals increasingly rely on digital platforms for communication, commerce, and information consumption, the need to safeguard personal data from unauthorized access and exploitation becomes paramount. In this context, the right to be forgotten emerges as a crucial mechanism for empowering individuals to assert control over their online identities and mitigate potential harms arising from the perpetual retention of digital footprints.

Additionally, the rise of algorithmic decision-making and automated content duration algorithms further complicates efforts to regulate online information dissemination and mitigate the impact of harmful or inaccurate content. As these technologies become increasingly pervasive, there is a growing imperative to establish transparent accountability mechanisms to ensure that algorithmic processes align with legal and ethical standards. This requires collaboration between policymakers, technologists, and civil society stakeholders to develop robust governance frameworks capable of promoting accountability, transparency, and fairness in digital content moderation. Thus, the interplay between digital and traditional media landscapes poses complex challenges for regulatory frameworks aimed at addressing issues of information removal and data privacy. By adopting a holistic approach that considers the multifaceted nature of contemporary media ecosystems, policymakers can develop adaptive regulatory frameworks capable of safeguarding individual rights while fostering innovation and digital inclusion.

Envisioning the personnel engaged in facilitating such a judicial decree and the logistical intricacies of information retrieval presents a formidable challenge. Moreover, even in the event of

purging all copies from library collections or periodical shelves, a complete and definitive "erasure" of information from the tangible world remains elusive. In such a scenario, the attainment of the applicant's objective through recourse to the right to be forgotten before the court becomes an exercise fraught with complexity and caution.

Indeed, if we extrapolate the unfolding circumstances to their logical conclusion, the next conceivable step would entail erasing the recollection of all individuals who have perused these publications and possess the potential to disseminate them – absent a legal injunction – thus assuming the role of information conduits. It becomes evident that in crafting potential scenarios, we risk delving into realms of absurd utopianism devoid of practical relevance, let alone feasibility or pragmatic implementation.

Expounding further on the practical implications of such hypothetical scenarios, it is essential to consider the broader societal and legal ramifications of attempts to erase or manipulate collective memory. Beyond the logistical challenges associated with purging information from physical archives and digital repositories, there exist profound ethical and philosophical questions concerning the nature of memory, truth, and historical preservation. Any attempt to selectively expunge or alter historical records raises fundamental questions about the integrity of historical narratives and the preservation of collective memory.

Moreover, the proliferation of digital technologies and the widespread dissemination of information through online platforms have exponentially compounded the challenges associated with information management and preservation. In an age characterized by the digitization of archival materials and the rapid circulation of information across digital networks, the task of controlling the flow of information and ensuring its accurate representation poses unprecedented challenges for legal and regulatory frameworks.

Furthermore, the erosion of privacy and the commodification of personal data by tech companies have raised concerns about the ethical implications of data retention and surveillance practices. As individuals increasingly rely on digital platforms for communication, commerce, and social interaction, the need to safeguard personal data from unauthorized access and exploitation becomes paramount. In this context, the right to be forgotten emerges as a vital mechanism for empowering individuals to exert control over their digital identities and mitigate the risks associated with prolonged data retention. So while the theoretical exploration of hypothetical scenarios involving the right to be forgotten may offer valuable insights into the complexities of information management and privacy protection, it is essential to temper such speculation with a pragmatic assessment of the practical challenges and ethical considerations involved. By fostering interdisciplinary dialogue and collaboration among legal scholars, ethicists, technologists, and policymakers, we can develop robust frameworks for addressing the multifaceted challenges posed by the digital age while upholding fundamental principles of justice, transparency, and individual rights.

These interconnected dialogues serve as the backdrop and narrative framework for the evolution and conceptualization of the Right to Be Forgotten (RTBF). They play a pivotal role in shaping the prevailing viewpoints and determining which perspectives are afforded visibility within the discourse. However they play a significant role in perpetuating preexisting disparities through the construction of knowledge within a “network society”. In this context, researchers view networks as inherently pluralistic and all-encompassing representations of societal dynamics. Consequently, perspectives that are already marginalized or lack influence may become further

marginalized and disenfranchised within this networked environment (Rebekah Larsen, 2020).[36]

Expanding on this discourse, it becomes evident that the construction of knowledge within a networked society is deeply intertwined with power dynamics and structural inequalities. The dissemination and circulation of information within digital networks are often shaped by dominant narratives and vested interests, thereby reinforcing existing power structures and marginalizing alternative perspectives. Moreover, the proliferation of digital technologies has led to the emergence of new forms of gatekeeping and information control, further exacerbating inequalities in access to knowledge and representation.

The conceptualization of the RTBF within this discursive framework underscores the importance of critically examining the ways in which digital technologies mediate access to information and shape public discourse. By interrogating the underlying power dynamics and structural inequalities inherent in knowledge production and dissemination, researchers can contribute to a more nuanced understanding of the RTBF and its implications for individual rights and societal dynamics.

Furthermore, the notion of visibility within digital networks raises important questions about the ethics of information dissemination and the responsibility of platform providers and policymakers in shaping public discourse. As digital platforms increasingly serve as primary conduits for accessing information and engaging in public debate, there is a growing need for transparency, accountability, and inclusivity in the governance of online spaces. Efforts to address issues of visibility and representation must therefore be accompanied by broader initiatives aimed at promoting digital

[36] Larsen, Rebekah. Mapping Right to be Forgotten frames: Reflexivity and empirical payoffs at the intersection of network discourse and mixed network methods. *New media & society*. Vol. 22 (7), (2020), 1250.

literacy, fostering media plurality, and safeguarding democratic values in the digital age. The intertwined discourses surrounding the RTBF underscore the complex interplay between technology, power, and knowledge within contemporary society. By critically examining these discourses and their implications for information access and representation, researchers can contribute to a more equitable and inclusive digital landscape that upholds the principles of justice, transparency, and democratic participation.

Another notable trend is the evolution of case law and judicial interpretation surrounding the right to be forgotten. European courts, including the Court of Justice of the European Union (CJEU) and national courts, have adjudicated numerous cases involving the right to be forgotten, providing guidance on its scope, limitations, and application in practice. These legal developments have contributed to a more nuanced understanding of individuals' rights in the digital realm and have established precedents for future cases.

Moreover, there is an ongoing discussion about the extraterritorial application of the right to be forgotten beyond the borders of the EU. As data flows transcend national boundaries, questions arise regarding the enforcement of European data protection standards globally and the interaction between the GDPR and laws in other jurisdictions. European regulators and policymakers continue to grapple with these complex issues as part of broader efforts to promote a consistent and harmonized approach to data protection on a global scale. In the last several years, these challenges have begun to have an impact on EU democracy support policies. To some degree, they have diluted the European commitment to democracy and human rights globally.[37]

[37] Recent Trends in EU Democracy Support. Toward a New EU Democracy Strategy, Sep. 1, 2019, pp. 3–10.

Overall, European trends in the development of the digital silence concept underscore the region's commitment to upholding individuals' privacy rights and promoting responsible data governance practices in the digital age. Through legislative initiatives, judicial decisions, and ongoing dialogue, Europe seeks to strike a balance between protecting privacy rights and fostering innovation and economic growth in the digital economy.

5. Conclusions

The ongoing digital revolution sweeping through society not only signifies advancements in technology but also heralds a reconfiguration of sociolegal dynamics, thereby complicating the realization and protection of human rights in the face of infringements, challenges, or denial. In the contemporary landscape, the proliferation of online platforms presents novel challenges, reshaping communicative norms and engendering the emergence of new information cultures while reshaping existing ones.

Moreover, the past decade has been pivotal not only for Ukrainian jurisprudence but also for legal discourse across Europe, marking a transformative shift from normative to interpretive legal paradigms. This epochal transition underscores the maturation of legal thought and the institutionalization of progressive legal principles. Central to this evolution has been the systematic integration of the right to digital silence and the right to be forgotten into the fabric of legal institutions, transcending boundaries and reshaping legal frameworks.

The maturation of these rights from theoretical constructs to actionable legal principles has been instrumental in galvanizing legal discourse and catalyzing judicial activism aimed at their practical implementation. This process has not only led to the delineation of socio-ideological and judicial criteria but has also witnessed a

proliferation of judicial decisions aimed at operationalizing these rights in real-world contexts.

As these rights continue to gain traction and permeate legal landscapes, it is imperative to examine their multifaceted implications for society, governance, and individual freedoms. Furthermore, ongoing scholarly inquiry and interdisciplinary collaboration are essential to navigate the evolving legal terrain and ensure the equitable protection of rights in the digital age. Thus, the integration of digital rights into legal frameworks represents a seminal moment in the evolution of jurisprudence, signaling a paradigm shift towards a more equitable and rights-centric legal order.

In conclusion, the concept of digital silence represents a complex and multifaceted phenomenon with wide-ranging implications for law, society, and ethics in the European context. By exploring its legal foundations, societal dynamics, and ethical considerations, this paper has provided a comprehensive analysis of digital silence and its significance in shaping the evolving landscape of digital rights and responsibilities in Europe. Moving forward, addressing the challenges posed by digital silence will require collaborative efforts from policymakers, regulators, technology providers, civil society actors, and individuals to uphold fundamental rights, promote digital literacy, and foster a more transparent, equitable, and rights-respecting digital ecosystem in Europe and beyond.

Contemporary Tendencies Regarding the Form and Procedure for Concluding Contracts

Kyrylo Anisimov*

Abstract: The author analyzes the main European values and their manifestation in the context of contract law. The author emphasizes the need to take them into account and further institutionalize them in the transition to a new formation of the information society to ensure sustainable development. In general terms, the author analyzes national civil legislation and practice regarding the form of a transaction, signature and, to some extent, the procedure for concluding a contract. Special research attention is devoted to the analysis of foreign experience on these issues, especially in countries that recognize or largely share the European values of contract law. The author supports the conclusions that it is advisable to use simplified procedures for concluding a contract while maintaining a balance between economic feasibility and the principle of freedom of contract. The author establishes that the requirement of a written form is intended to ensure sufficient formalization and objective expression of the content of the transaction, and the signature is intended to identify the party to the contract, to certify its personal participation in signing and to demonstrate its agreement with the content of the contract. The author notes that the signature function may be fulfilled by authentication of a party to a contract. Thus, a flexible approach can be applied to the signature, depending on the nature of the parties' activities; trade and business customs; availability of alternative methods of counterparty identification and recognition of such methods in practice; other legal, commercial and technical factors. Therefore, the author emphasizes the main ways to further improve the current Ukrainian legislation to meet the needs of today and to comply with the basic European values.

* *PhD, Assistant Professor of Department of Civil Procedure, Arbitration and Private International Law of Yaroslav Mudryi National Law University, Kharkiv, Ukraine. K.g.anisimov@nlu.edu.ua*

Keywords: European values; freedom; equality; principles of law; private law; international private law; contract law; form of contract; written form; electronic form; signature; procedure for concluding a contract; simplified procedure for concluding a contract

1. Information society and the values of contract law

With the onset of the information technology revolution, entirely logical and organic processes of transition of the foundations of our society began. Overall, we can confidently state that we have witnessed a gradual transition to a new formation – the information society.

In our opinion, O. G. Danilyan and O. P. Dzoban characterize the information society from the legal reality perspective quite exhaustively by highlighting the following features:

1. Information becomes the main economic resource and the information sector takes the first place in terms of development, number of employees, and share of investments.

2. There is a developed infrastructure that ensures the creation of sufficient information resources. The main form of capital is intellectual property.

3. Information becomes a subject of mass consumption through the mass media system. The information society provides any individual with access to any source of information, which is guaranteed by law and technical capabilities. The legal basis of the information society is being developed.

4. A new worldview is being formed, in which virtual values play a significant role. This leads to the transformation of traditional moral norms of a prohibitive and permissive nature, to the emergence of moral conflicts and conflicts that have a significant impact on the spiritual and moral world of a person, his or her self-identification.

5. Business activity and the culture of communication in general are transferred to the information and communication environment, resulting in the formation of virtual spheres of life in society (economy, politics, education, law, etc.), which give rise to a new type of virtual worldview that defines a specific system of moral values of a symbolic and simulative nature[1].

Meanwhile, this transition to new formations in developed countries is not chaotic. It is characterized by rapid but sustainable development. To a large extent, such sustainability is achieved through the existence of clearly articulated and distinguished values common to a particular society. And here it is necessary to emphasize that such values, and especially European values, are not some purely abstract phenomena.

Thus, in accordance with the provisions of the article 2 of the Lisbon Treaty the European values are human dignity, freedom, democracy, equality, the rule of law and human rights[2]. These values are not only common for all Member States of the European Union, but the one of European Union major aims is to promote such values[3].

At the same time, such values as human dignity, freedom, equality and solidarity, as well as the principles of democracy and the rule of law are the basis for the Charter of Fundamental Rights of the European Union[4]. In particular, it enshrines the principles, rights and freedoms that are basic not only to public but also to private law.

[1] Данильян, О. Г., Дзьобань, О. П., Трансформації цінностей в інформаційному суспільстві: багатовимірність та різнопорядковість. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*, 3(46), 2020, С. 29–30.

[2] Consolidated Versions of The Treaty on European Union and The Treaty on The Functioning of The European Union (2016/C 202/01).

[3] Consolidated Versions of The Treaty on European Union and The Treaty on The Functioning of The European Union (2016/C 202/01).

[4] Charter of Fundamental Rights of the European Union (2012/C 326/02).

If we are talking about private law, and more specifically about contract law, then it is to a greater extent based on the values of freedom and equality that find the most traction among other values in specific legal principles and norms. In particular, one of the main principles is the principle of freedom of contract. In general, the doctrine of freedom of contract stipulates that counterparties should be free to settle their mutual relations without state interference[5]. It means that the parties are free to determine the terms of the contract, the form of the contract, etc., taking into account the requirements of civil law, business practices, and the requirements of reasonableness and fairness.

The development and emergence of massive IT markets have had a significant impact on the mechanisms of contracting. In particular, the use of contracts with a simplified procedure for concluding them is now widespread in legal practice. At the same time, this creates certain challenges for the reconceptualization of the basic provisions of contract law in the context of the need to further liberalize civil law and protect the freedom of contract and the autonomous will of the parties from external interference.

In general, the consent of the parties is the fundamental attribute of such a civil law category as a "contract". Reaching an agreement as the final product of the parties' will is not possible without the respective wills of the counterparties. Such expressions of will are a proposal to enter into an agreement (offer) and acceptance of the offer (acceptance). At the same time, in order for a civil law contract to be considered concluded, the parties' will must be expressed in a certain form.

[5] D. D. Barnhizer, *Bargaining Power in Contract Theory*. *Visions of Contract Theory: Rationality, Bargaining and Interpretation*. Legal Studies Research Paper / L. A. DiMatteo, R. A. Prentice, B. D. Morant and Daniel D. Barnhizer, eds. Durham, North Carolina: Carolina Academic Press, 2007. P. 101.

2. Analysis of the current state of Ukrainian legislation

Article 205(1) of the Civil Code of Ukraine provides for the following possible forms of transactions: oral and written (electronic)[6]. If we analyze in detail the provisions of Chapter 16 "Transactions" and Chapter 53 "Conclusion, Amendment and Termination of a Contract" of the Civil Code of Ukraine, we can conclude that Ukrainian civil law provides for the fiction of a written form for electronic contracts. In particular, this is clearly indicated by the provision of Article 639(2)(2) of the Civil Code of Ukraine, namely, if the parties agree to enter into an agreement by means of information and communication systems, it shall be deemed to be in writing.

However, in Article 6(2) of the Law of Ukraine No. 959-XII dated 16.04.1991 "On Foreign Economic Activity" the legislator separately identifies the electronic form of the agreement along with the written form[7]. However, the main act of civil legislation is the Civil Code of Ukraine. So, its provisions have a hierarchical priority over the provisions of other regulatory legal acts in the relevant areas[8]. Thus, in accordance with the decision of the Civil Court of Cassation dated 17.11.2021 in case No. 172/1159/20, oral and written (electronic) forms of transactions are currently provided for[9]. In this decision, the court defined the category "form of transaction" and explained that the form of transaction means a way of expressing the will of the party (parties) and/or fixing it. These positions were supported by the decision of the Joint Chamber of the Civil Court of Cassation dated 18.05.2022 in case No. 393/126/20[10]. At the same time, they were also

[6] Цивільний кодекс України: Закон України від 16.01.2003 р. No 435-IV.

[7] Про зовнішньоекономічну діяльність: Закон України від 16.04.1991 № 959-XII.

[8] В. Крат, *Значення договору в приватному праві крізь призму практики ВС. Закон і Бізнес.* 13 червня 2022 року.

[9] Постанова КЦС ВС від 17.11.2021 р., справа No 172/1159/20.

[10] Постанова ОП КЦС ВС від 18.05.2022 р., справа No393/126/20 .

supplemented by the statements that a transaction is formalized by fixing the will of the party (parties) and its content, as well as such fixation shall be carried out in various ways.

However, the issues of the correlation between written and electronic forms and the degree of independence of the latter remain open still. Thus, the authors of the Concept for Updating the Civil Code of Ukraine proposed to revise the general approaches to the form of a transaction and to determine the range of transactions that should be made in writing, in electronic form (taking into account its specifics and the role of the electronic digital signature) and orally (taking into account technical advances in data transmission)[11].

L. R. Katynska, drew attention in her dissertation to the fact that the Ukrainian legislator, when amending Article 205 of the Civil Code of Ukraine, laid down an expanded approach to understanding the written form of a transaction, which is not consistent with the two-tier approach common in the EU member states[12]. According to the latter, only a qualified electronic expression of will, i.e. one signed with a digital signature with a valid qualified key certificate, is equated with a written form.

Extending this idea, we consider that the general fiction of the written form for contracts concluded through information and telecommunication systems established in Article 639(2)(2) of the Civil Code of Ukraine and the mandatory requirement of Article 207(2)(1) of the Civil Code of Ukraine that the parties to a contract sign the contract in order for the contract to be considered concluded in writing are somewhat inconsistent. Thus, the signatures of the counterparties are mandatory requisites of

[11] Концепція оновлення Цивільного кодексу України. Київ: Видав. дім "АртЕк", 2020. С. 11–12.

[12] Л. Р. Катинська, *Електронна форма правочину (порівняльний аналіз правового регулювання в Україні та Польщі)*: дис. … канд. юрид. наук. Тернопіль, 2017. С. 43–44.

an agreement concluded in writing. At the same time, pursuant to Article 207(3) of the Civil Code of Ukraine, a facsimile reproduction of a signature by means of mechanical, electronic or other copying, electronic signature or other analog of a handwritten signature may be used in transactions. Such use is permitted in cases established by law, other acts of civil law, or by written agreement of the parties, which must contain samples of the respective analog of their handwritten signatures, or otherwise regulate the procedure for its use by the parties.

Also, we would like to draw attention to the Law of Ukraine "On Electronic Documents and Electronic Document Management" No. 851-IV dated May 22, 2003. Pursuant to Article 6 of this Law, the creation of an electronic document is completed by the imposition of an electronic signature that can be used to identify the author of the electronic document[13]. At the same time, the relations related to the use of advanced and qualified electronic signatures are regulated by the Law of Ukraine "On Electronic Trust Services"[14], and the use of other types of electronic signatures in electronic document management is carried out by electronic document management entities on a contractual basis. At the same time, Article 8 provides that the legal force of an electronic document cannot be denied solely because it is in electronic form.

Moreover, we believe that it is also advisable to analyze some provisions of the Law of Ukraine "On Electronic Commerce" No. 675-VIII dated September 03, 2015[15]. Article 12 of this Law is of particular interest. According to its provisions, if, in accordance with an act of civil law or by agreement of the parties, an electronic transaction is to be signed by the parties, the moment of its signing

[13] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV.

[14] Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII.

[15] Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII.

is the use of: 1) an electronic signature or an electronic digital signature in accordance with the Law of Ukraine "On Electronic Digital Signature", provided that all parties to the electronic transaction use an electronic digital signature; 2) an electronic signature with a one-time identifier defined by this Law; 3) an analog of a handwritten signature (facsimile reproduction of a signature by means of mechanical or other copying, other analog of a handwritten signature) with the written consent of the parties, which must contain samples of the respective handwritten analogs.

The Law of Ukraine "On Electronic Commerce" defines an electronic signature with a one-time identifier as data in electronic form in the form of an alphanumeric sequence attached to other electronic data by a person who has accepted an offer to enter into an electronic agreement and sent to the other party to the agreement. However, with regard to the term "electronic signature", there is a note that it is used in the meaning given in the Law of Ukraine "On Electronic Digital Signature".

Firstly, it should be noted that the Law of Ukraine "On Electronic Digital Signature" dated 22.05.2003 No. 852-IV has been repealed by the Law "On Electronic Trust Services" dated 05.10.2017 No. 2155-VIII. Secondly, although the Law of Ukraine "On Electronic Digital Signature" provided a definition of an electronic signature, this Law only defined the legal status of an electronic digital signature (in particular, the list of conditions when an electronic digital signature is equivalent to a handwritten signature in terms of legal status) and regulated relations arising from the use of an electronic digital signature only. Finally, the imperfection of the legislative wording of paragraph 2 of Article 12 of the Law of Ukraine "On Electronic Commerce" is obvious, as domestic researchers have already pointed out. These provisions can be interpreted as an actual equalization of the legal force and legal status of an electronic signature and an electronic digital

signature, and as recognition of the possibility for an electronic digital signature to be analogous to a handwritten signature in terms of legal consequences only[16].

One of the main principles underlying the above-mentioned Law of Ukraine "On Electronic Trust Services" is the creation of favorable and competitive conditions for the development and functioning of the electronic identification sector. In this Law, electronic identification means the procedure for using a person's identification data in electronic form that uniquely identifies an individual, legal entity or representative of a legal entity. The Law also defines an electronic signature as electronic data that is added by the signatory to other electronic data or is logically linked to them and used as a signature. At the same time, the legislator no longer uses the term "electronic digital signature". Instead, the concepts of "advanced electronic signature" and "qualified electronic signature" have been introduced. An advanced electronic signature is an electronic signature created as a result of cryptographic transformation of electronic data to which this electronic signature is linked, using an advanced electronic signature tool and a personal key uniquely associated with the signatory, and which allows for electronic identification of the signatory and detection of violations of the integrity of the electronic data to which this electronic signature is linked. In turn, a qualified electronic signature is an advanced electronic signature created using a qualified electronic signature tool and based on a qualified public key certificate.

3. Analysis of foreign legislation and experience

First of all, let's pay attention to the relevant provisions of the UNCITRAL Model Law on Electronic Commerce regarding the form

[16] Н. Ю. Філатова, *Правочини з використанням електронної форми представлення інформації. Проблеми законності*. 2017. Вип. 136. С. 50–51.

and procedure for concluding contracts[17]. Pursuant to Article 11 of the Model Law, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose. In this case, a data message should be understood as information that is prepared, sent, received or stored by electronic, optical or similar means, including, but not limited to, electronic data interchange, e-mail, telegram, telex or telefax. At the same time, Article 6 proposes that the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

It should be noted that the United Nations Convention on the Use of Electronic Communications in International Contracts contains legal rules that are quite similar in content[18]. First of all, according to Article 8 of the Convention, A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication. And Article 9(2) states that where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference. At the same time, pursuant to Article 9(3), where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if: (a) A method is used to identify

[17] UNCITRAL: Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.

[18] United Nations Convention on the Use of Electronic Communications in International Contracts. United Nations publication.

the party and to indicate that party's intention in respect of the information contained in the electronic communication; and (b) The method used is either: (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

The modern US legislation on the form of transactions was significantly influenced by the English Statute of Frauds of 1677. It is worth noting that this statute required a written form and mandatory signatures of the parties for certain types of contracts in order to avoid fraud in court through false testimony[19]. This practical purpose of the written form of the contract and signature remains unchanged today. In view of this, the provisions of the statute of frauds were introduced into the Uniform Commercial Code of the United States (UCC), which has been adopted by all states except New York and South Carolina.

However, in the United States, the National Conference of Commissioners on Uniform State Laws (NCCUSL) prepared the Uniform Electronic Transactions Act (the "UETA") and the Uniform Computer Information Transactions Act (the "UCITA") for electronic transactions. It should be noted that the NCCUSL Uniform Laws are not legally binding in themselves until they are adopted in the state through a specific procedure.

In general, the UETA covers a wide range of transactions and is intended to significantly facilitate the procedure for concluding contracts in electronic form[20]. According to paragraph 102(8) of the UETA, an electronic signature for the purposes of the law means

[19] Statute of Frauds: 1677 Chapter 3 29 Cha 2.

[20] Uniform Electronic Transaction Act: Uniform Act proposed by the National Conference of Commissioners on Uniform State Laws. 1999.

an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record. The legal significance of such a signature is determined taking into account the context and objective circumstances at the time of its creation, execution or acceptance. In other words, a separate parallel regime of existence is not created for an electronic signature. Thus, the electronic form of an agreement is considered appropriate for all cases where the law requires a written form.

At the same time, UCITA applies only to contracts and transactions involving "computer information", but regulates all related aspects[21]. In terms of signing a contract, UCITA uses the term "authenticate", not "electronic signature". Authentication requires (1) signing or (2) otherwise performing or accepting a symbol or sound, or using encryption or other process with respect to data, with the intention of the authenticating person: to identify that person; to accept the terms and conditions reflected in the data; or to confirm the content of the information in the data. At the same time, paragraph 119(c) actually establishes a presumption of the intention to authenticate a person. First of all, this provision was aimed at intensively stimulating the development of mass markets for intellectual property rights through further simplification of signing contracts in electronic form.

It is worth noting that the provisions of UCITA have been significantly criticized by scholars as significantly upsetting the balance of rights and obligations of the counterparties[22]. After all, the uniform approach to different types of electronic signatures used in the UETA and the absence of technical requirements for

[21] Uniform Computer Information Transactions Act: Uniform Act proposed by the National Conference of Commissioners on Uniform State Laws. 1999.

[22] B. D. Macdonald, *Contract Enforceability: The Uniform Computer Information Transaction Act,* in *Berkeley Technology Law Journal*, Vol. 16, 2001, P. 461.

them have already greatly simplified the conclusion of contracts in electronic form. Moreover, as G. L. Founds emphasizes, UCITA was not able to resolve conflicts between US federal law and the contract law of individual states[23]. As a result, while the UETA was adopted by 48 states, the District of Columbia and the Virgin Islands of the United States, the UCITA was adopted only by the states of Virginia and Maryland.

The framework rules for the use of electronic signatures by EU Member States were presented in Directive 1999/93/EC of the European Parliament and of the Council of the European Union on a Community framework for electronic signatures of December 13, 1999[24]. We would like to emphasize that, in accordance with the provisions of the Directive, a simple electronic signature is legally binding, since the legal effect of its use when signing a document cannot be leveled by expressing one's will in electronic form. At the same time, in case of a requirement for mandatory handwritten signing of a certain agreement in national legislation, according to Article 5(1)(a), such a requirement should be considered fulfilled if an advanced electronic signature based on a valid certificate and created using secure signature creation mechanisms is available. Thus, based on the analysis of the provisions of this Directive, it can be concluded that it, along with the above-mentioned United Nations Convention on the Use of Electronic Communications in International Contracts, laid down a rather flexible approach to signing contracts with electronic signatures at that time.

However, Directive 1999/93/EC has lost its legal force due to the entry into force of Regulation No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic

[23] G. L. Founds, *Shrinkwrap and Clickwrap Agreements: 2B or Not 2B?,* in *Federal Communications Law Journal*, Vol. 52, Iss. 1, 1999, P. 100–101.

[24] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[25]. It should be emphasized that in accordance with Article 288 of the Treaty on the Functioning of the EU, the provisions of the Regulation are directly applicable in the EU, and the provisions of the national legislation of the EU Member States do not apply to the extent that they contradict the Regulation[26]. At the same time, Article 2(3) of the Regulation states that it does not affect national or Union law relating to the conclusion and validity of contracts or other legal or procedural obligations related to form. In general, Regulation No. 910/2014 establishes the conditions under which Member States recognize the means of electronic identification of natural and legal persons covered by a notified electronic identification scheme of another Member State; rules on trust services; legal framework for electronic signatures, etc. Thus, such types of electronic signatures as electronic signature, advanced electronic signature and qualified electronic signature are enshrined. It is worth noting that many provisions of Regulation No. 910/2014 were used as the basis for the Law of Ukraine "On Electronic Trust Services" in order to harmonize the relevant Ukrainian legislation with EU law.

The provisions of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")[27] remain the starting point for the relevant national legislation of the EU Member States. Thus, one of the main requirements of the

[25] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[26] Consolidated version of the Treaty on the Functioning of the European Union.

[27] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Directive is to ensure that EU Member States in their legal systems allow for the conclusion of contracts by electronic means. The conclusion process itself must be ensured in such a way as not to create obstacles for the parties to use contracts in electronic form, and the conclusion of a contract in electronic form cannot result in its loss of legal force. It should be noted that the Directive sets out a minimum list of information that must be provided when concluding a contract in electronic form, namely: various technical measures on the way to concluding the contract; whether the contract will be accepted by the service provider and whether it will be accessible; technical means of identifying and correcting input errors before the request is placed; languages offered for concluding the contract.

As Jane K. Winn and Jens Haubold fairly underline, the Directive was based on the principle of "contract law neutrality"[28]. That is, the Directive was created as a legal instrument that does not control the process of concluding a contract in full, but provides for such rules that will not significantly affect the existing rules of national contract law of the EU Member States, in particular, the form of the contract and the procedure for its conclusion[29]. For example, the provisions of the Directive do not contain the terms "offer" and "acceptance". After all, what in Danish or Spanish civil law is a full-fledged proposal to enter into a contract with all the relevant legal consequences, as Sylvia Kierkegaard aptly explains, in English law is only an invitation to make an offer[30]. At the same time, Arno R. Lodder writes that initially the text of the draft proposal referred to the process of concluding contracts in

[28] J. K. Winn, J. Haubold, *Electronic promises: contract law reform and e-commerce in a comparative perspective*, in *European Law Review*, Vol. 27, 2002, P. 574.

[29] C. Riefa, *The reform of electronic consumer contracts in Europe: towards an effective legal framework?,* in *Lex Electronica*, Vol. 14, No. 2, 2009. P. 7.

[30] S. M. Kierkegaard*, E-Contract Formation: U. S. and EU Perspectives*, in *Washington Journal of Law, Technology & Arts*, Vol. 3, Iss. 3, 2007.

electronic form, but later this wording was abandoned due to the objective impossibility of quickly reaching a consensus on such an issue[31]. In general, European researchers are inclined to believe that this decision was justified not so much by legal needs, but rather by the EU's political strategy, which consisted of deliberate abstention due to difficulties in harmonizing the national contract law of the EU member states[32].

In terms of the issue under study, it should be noted that the Resolution of May 26, 1989 proclaimed the need for gradual harmonization of the private law of the EU Member States[33]. In view of this, in recent decades, the EU has made many attempts to unify civil law. One of the most ambitious projects was the development of the European Union Civil Code. The work "Towards a European civil code", which was first published in 1994 and included the work of leading researchers on social issues, economic analysis of private law, the future of e-commerce, arguments in favor of and against a single European Civil Code, was crucial in this regard[34]. A landmark event was the publication of the Principles of International Commercial Contracts or UNIDROIT Principles in 1994. Subsequently, the Commission on European Contract Law (also known as the Lando Commission), which was established by Ole Lando, presented the Principles of European Contract Law to the European legal community[35]. At the same time, the Study Group on a European Civil Code, the Research Group on EC Private

[31] A. R. Lodder, *European Union E-Commerce Directive – Article by Article Comments: Guide to European Union Law on E-Commerce*. Update from 2016 (published 2017) of the 2001 (published 2002) version, published in EU Regulation of E- Commerce. Camberley, Surrey: Edward Elgar Publishing, 2017. Vol. 4.

[32] J. K. Winn, J. Haubold, *Electronic promises: contract law reform and e-commerce in a comparative perspective*, cit., P. 574.

[33] Resolution on action to bring into line the private law of the Member States.

[34] M. Hesselink, A. Hartkamp, E. Hondius, E. Perron, M. Veldman, C. Joustra, et al. *Towards a European civil code*. 3rd ed. Kluwer Law International, Amsterdam, 2004.

[35] Principles of European Contract Law – PECL.

Law or the Acquis Group, etc. started their work around this time. Thus, the result of more than twenty years of work and one of the most significant scientific achievements in the field of unification of European private law today is the Draft Common Frame of Reference: Principles, Definitions and Model Rules of European Private Law (hereinafter – "DCFR")[36].

Of course, the Draft Model Rules do not contain any directly applicable rules, but they contain provisions that summarize the best legal practices of European countries and a number of innovations. First of all, the DCFR stipulates that when a contract is concluded by electronic means, the party that proposed the terms and conditions that were not specifically agreed upon may refer to them in relations with the other party when they are communicated to such party in the form of a text. In this case, the terms and conditions must be available for review in the future within a reasonable period of time. However, the most important provisions of the DCFR for contracts with a simplified procedure for concluding, namely for wraparound license agreements, are those related to signatures. Specifically, the author argues that a signature is not required to comply with the written form of the agreement. At the same time, it has been established that a reference to a person's signature includes a reference to that person's handwritten signature, electronic signature or advanced electronic signature, as well as a reference to anything signed by a person, should be interpreted accordingly. We would also like to emphasize that the DCFR recognizes that different types of signatures provide different types of identification of counterparties. However, a signature is not a mandatory requisite of the written form of a contract, and when a general requirement for a signature is made (without specifying a particular type), both

[36] Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR).

a person's handwritten signature and a simple electronic signature are acceptable.

In German civil law, the electronic form is a separate and independent type of form in which a transaction can be made. While the provisions on the written form are set forth in Section 126 of the German Civil Code, the corresponding provisions on the electronic form are set forth in Section 126a[37]. At the same time, pursuant to Section 126a of the German Civil Code, an electronic form may replace the written form required by law if the person who made the notification indicates his or her name and signs the electronic document with a qualified electronic signature in accordance with the Electronic Signature Act (Signaturgesetz). Thus, we can see that written and electronic forms are clearly distinguished, but if there is a legal requirement that the written form of an agreement be binding, the electronic form is acceptable under certain conditions.

It is noteworthy that Section 126b of the German Civil Code emphasizes the textual form of a transaction. Thus, a legible communication with the name of the person making it must be on a durable medium. The law defines a durable medium as one that 1) allows the recipient to retain a message addressed to him personally for as long as it is relevant, and 2) allows such a message to be reproduced without changes. Hence, it can be unequivocally concluded that the message does not have to be materialized on paper, but can be expressed by various technical means, in particular, information and telecommunication systems. In support of this, we note that Section 312c of the German Civil Code provides for a textual form for contracts concluded remotely. In general, the textual form is sufficient for contracts

[37] Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 14. März 2023 (BGBl. 2023 I Nr. 72) geändert worden ist.

with a predominantly informational component and may serve as a simple written form without the parties' signature. However, when entering into a contract in textual form, the following must be ensured: 1) the possibility of identifying the parties and 2) the possibility of determining the subject matter of the agreement and its content[38]. There is no separate procedure for identifying the counterparty, and therefore, the proper data for an individual is his or her name, and for a legal entity – the name.

4. Concerning the issue of standard forms and simplified procedures for concluding contracts

Undoubtedly, the emergence of massive technology markets and the transition to an information society have determined the need to optimize contractual forms and procedures. But at the same time, this has given rise to a lot of debate about the need to strike a balance between economic feasibility and the principle of freedom of contract.

Thus, professor Margaret Jane Radin argues that standardized forms of contracts in mass markets directly limit the rights of users to voluntarily agree to the terms of contracts. In her work "Boilerplate: The Fine Print, Vanishing Rights And The Rule Of Law", the scientist describes two archetypal dimensions of the existence of contracts: World A and World B[39]. Contracts in World A are transactions between two parties based on the principle of freedom of contract and in which each party agrees voluntarily. Typical for these contracts is the presence of negotiations between the parties, which contributes to the satisfaction of their interests. At the same time, the researcher characterizes contracts from World B as those that are concluded without

[38] F. Breuer, *Der Unterschied zwischen Schriftform und Textform*.

[39] M. J. Radin, *Boilerplate: The Fine Print, Vanishing Rights and the Rule of Law*, Princeton University Press, Princeton, 2013, P. 3, 9–12, 14, 19.

actual consent, since the user is not aware of such a conclusion or, at least, cannot do anything about it. World B is the dimension of templates and standard forms that gradually narrow legal rights until they disappear completely. Thus, M. J. Radin argues that standard adhesion agreements lack the necessary elements of a contractual transaction and free choice by the user, and therefore are only "purported contracts". She calls the absence of voluntary consent, in her opinion, "normative degradation". In addition, the author criticizes scholars and legal practitioners who defend archetypal World B contracts for including these contractual forms in the World A contractual consent paradigm. She also points out the complexity of the legal language in the studied contracts and the associated unfair conditions that can keep the user in the dark and thus create an imbalance in favor of the other party.

Another researcher Robert P. Merges was also concerned about the growing popularity of simplified contractual forms, as he believed that contractors would face the problem of truncation of contractual freedom, which would consist in the absence of a real choice of contract terms[40]. In his opinion, standardized forms of contracts in the industry determine further unification and similarity of contract terms. Such processes in the future may threaten the gradual formation of "private legislation".

The concept of "private legislation" as a negative characteristic of the global trend towards the widespread use of the legal structure of adhesion contracts in the twentieth century was introduced by Friedrich Kessler in 1943. The scientist studied the practice of using uniform contractual terms in various industries and concluded that a sharp increase in the identity of such terms indicates a regression of contract law. This is also a kind of starting

[40] R. P. Merges, *The commercial law of intellectual property*, in *Michigan Law Review,* Vol. 93, 1995, P. 1609.

point for the dominance of status and standard form over the very essence of the contract and the coherence of the will of its parties[41]. F. Kessler believed that contracts of adhesion, standard forms and uniform contractual terms have a powerful potential to become an effective and dangerous mechanism in the hands of global industrial and commercial unions, allowing them to further impose an authoritarian contractual order.

However, it should be realized that at that time many scholars shared a different point of view regarding adhesion agreements and standard forms in general and, in particular, boxed wrap license agreements. First of all, the position of Karl N. Llewellyn, one of the drafters of the Uniform Commercial Code of the United States and a prominent representative of the legal realism school, on standard contracts. He developed the concept, that a party that joins a standard contract almost never agrees to all its terms, but as long as such terms are not manifestly unfair in content or form, the judicial system should help ensure their proper implementation if the parties have entered into a contract[42].

Another scholar, David W. Slawson, drew attention to the fact that already in the 1970s, contracts using the legal structure of adhesion accounted for almost ninety-nine percent of all contracts concluded, and therefore the vast majority of people would find it difficult to remember when they entered into a contract not in the standard form[43]. Researchers from Washington and Lee University noted that contracts with a simplified conclusion procedure were already the most popular method of software licensing in the

[41] F. Kessler, *The contracts of adhesion – some thoughts about freedom of contract role of compulsion in economic transactions*, in *Columbia Law Review*, Vol. 43, 1943, P. 631.

[42] K. N. Llewellyn, *What Price Contract? – An Essay in Perspective*, in *The Yale Law Journal*. Vol. 40, No. 5, 1931.

[43] W. D. Slawson, *Standard form contracts and democratic control of lawmaking power*, in *Harvard Law Review*, Vol. 84, No. 3, 1971, P. 529.

computer industry as of 1985, precisely because it was impractical to obtain a signature from each contractor[44].

Finally, in any case, the standardization of contract forms and the use of simplified procedures for concluding contracts perform the same function as the standardization of goods and services in modern society, given that they are integral components of the mass production system.

5. Final thoughts

Basically, the researcher M. A. Eisenberg noted that in the twenty-first century, the rationale for contract law should be individualized, not standardized; subjective, not objective; multifaceted, not binary; and dynamic, not static[45]. We fully agree with this statement and believe that further reform of Ukrainian private law should be based on such principles, as well as taking into account European values. After all, as the above analysis of the current provisions of domestic civil law has shown, there are still many conflicts and gaps in the issues related to the form of the contract. In particular, the provisions of the DCFR may serve as a kind of guideline. It is true that they remain largely compromise, given the diversity and numerous differences in European national legal systems. However, the DCFR remains a progressive model that demonstrates an appropriate level of flexibility, dynamism and efficiency of legal regulation, in particular with regard to signatures as a civil law category.

In further scientific research of this issue, it is necessary to realize that the meaning of the written form and signature in civil law, although interrelated, is somewhat different. If the written

[44] *The Protection of Computer Software Through Shrink-Wrap License Agreements*, in *Washington and Lee Law Review*, Vol. 42, Iss. 4, Art. 11, 1985, P. 1360.

[45] M. A. Eisenberg, *The Emergence of Dynamic Contract Law*, in *California Law Review*. 2000 Vol. 88, No. 6, P. 1744–1745.

form primarily provides sufficient formalization of the content of the transaction on which the parties have agreed, the signature identifies the counterparties, ensures the certainty of their personal participation in the act of signing and demonstrates their agreement with the content of the contract. the presentation of data in writing is a kind of initial requirement and should not be mixed with the presentation of a signed written document.

A simple written or electronic form requires further research in domestic civil law and proper consolidation. At the same time, a flexible approach should be applied to the issue of signature, taking into account the nature of the parties' activities, trade and business customs, the availability of alternative methods of identifying counterparties and the recognition of such methods in practice, the balance between reliability and real market needs, as well as other legal, commercial and technical factors.

Theme 3
Procedural aspects of the implementation of European fundamental values in the digital era

Ensuring the Right to a Fair Trial Through the Use of Information Technology in Civil Procedure

Nataliia Sakara*

Abstract:The article is dedicated to the topic of the observance of the right to a fair trial when information technologies are employed in civil proceedings. The author, having analysed the judgments of the European Court of Human Rights which raised the issue of a violation of Article 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms when using information technologies, attempts to determine which components of the right to a fair trial may be violated and under what conditions. Furthermore, the author provides and evaluates the latest case law of the Supreme Court on this issue.

The author establishes that in order to ensure the right of access to court, Ukraine provides for the possibility of applying to court both by sending documents in paper and electronic form. The use of the latter has peculiarities depending on the specifics of the person exercising his/her right to go to court. As a general rule, documents in electronic form should be sent after registration of an electronic cabinet in the Unified Judicial Information and Telecommunication System only using its subsystems. At the same time, only individuals retain the right to send appeals to the official court e-mail. Regardless of the method of sending documents, they must be signed with an electronic digital

* *Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of International, Civil and Commercial Law of the State University of Trade and Economics, Judge of the Cassation Civil Court of the Supreme Court, Kyiv, Ukraine. E-mail: sakaranatasha@gmail.com*

signature, which must be verified by court employees. At the same time, in practice, there are some peculiarities of electronic filing that are not inherent in paper filings.

In order to ensure the right to a fair trial, in addition to the traditional methods of notification, it is also allowed to send a notice to the electronic cabinet of a party to a case, and under certain conditions, by placing an announcement on the official website of the judiciary. At the same time, the author expresses his own opinion that the "presumption of awareness" formulated in a number of Supreme Court judgments, although not provided for by national legislation, may ensure proper notification of the parties to the case, since the latter, by informing the court of their email address to which they may receive notices, thereby agree to receive them in this way, although they are not obliged to do so. At the same time, as a general rule, notifications by means of a telephone message, SMS message, or messenger messages are not considered to be proper.

It is stated that videoconference hearings are increasingly being used in the current environment, thereby ensuring the right to a public hearing if the parties to the case are not able to be directly present in the courtroom. At the same time, this format of the case hearing has certain peculiarities which were analysed by the author.

The author comes to the conclusion that the current procedural legislation and law enforcement practice are gradually increasingly using information technologies in civil proceedings. Despite the existing problems, national courts are trying to take into account the ECHR case-law on the right to a fair trial as much as possible.

Keywords: right to a fair trial; information technology; Unified Judicial Information and Communication System; electronic cabinet; submission of documents to the court in electronic form; notification by e-mail specified by a party to the case; presumption of awareness; notification of participants by placing an announcement on the official website of the judiciary; access to electronic case materials; trial by video conference

1. Introduction

The coronavirus lockdown, along with further Russian aggression against Ukraine and the imposition of martial law, has led to a rethinking of many everyday things in everyone's life. One of the main challenges of modern Ukrainian society is to adapt the way of life to modern realities, which means, on the one hand, ensuring maximum security measures, but at the same time maintaining the ability to fulfil everyday needs in a regular way.

The judicial system is no exception. Courts are faced with the task of administering justice in conditions of "limited contact" between the parties to a case, but at the same time with maximum preservation of traditional values of justice and ensuring human rights. This has been one of the driving forces behind the more active digitalization of judicial proceedings and the use of various modern information technologies at the national level, the usefulness of which has long been recognized by the international community. For example, in Recommendation No. R (84) 5 of the Committee of Ministers of the Council of Europe to member states on the principles of civil procedure designed to improve the functioning of justice, adopted by the Committee of Ministers on 28 February 1984 at the 367th meeting of Ministers' Deputies, it was explicitly stated that "the most modern technical means should be made available to the judicial authorities so as to enable them to give justice in the best possible conditions of efficiency, in particular by facilitating access to the various sources of law and speeding up the administration of justice" (Principle 9)[1]. Subsequent recommendations of the Committee of Ministers to the Council of Europe identified areas of the judiciary and related

[1] Recommendation No. R (84) 5 of the Committee of Ministers of the Council of Europe to member states on the principles of civil procedure designed to improve the functioning of justice, adopted by the Committee of Ministers on 28 February 1984 at the 367th meeting of Ministers' Deputies. *International standards in the field of justice*. K.: Istyna, 2010. 302.

institutions where the prospective introduction of information technology would have a positive impact on overall efficiency[2].

On 01.12.2023, the Consultative Council of European Judges (CCEJ), building on its previous opinions and taking into account relevant Council of Europe instruments and other documents, adopted Opinion No. 26 (2023) "Moving forward: the use of assistive technologies in the judiciary". It reiterates "the importance of developing and using technology in ways that maintain and, where possible, enhance the fundamental principles of the rule of law". It emphasizes that "States are required to secure effective and practical access to justice. Technology is a medium through which they can do so, both in the ordinary course of events and in extraordinary or emergency circumstances. It is thus one of the means through which a democratic state, committed to securing the rule of law, can enable the judicial power of the state to be exercised at all times". At the same time, the administration

[2] Recommendation № R (95) 11 of the Committee of Ministers of the Council of Europe to member states concerning the selection, processing, presentation and archiving of court decisions in legal information retrieval systems (adopted by the Committee of Ministers on 11 September 1995 on the 543 meeting of Ministers' Deputies). *European and international standards in the field of justice.* K, 2015. 242–248; Recommendation Rec (2001) 2 of the Committee of Ministers of the Council of Europe to member states concerning the design and re-design of court systems and legal information systems in a court-effective manner (adopted by the Committee of Ministers on 28 February 2001 on the 743 meeting of Ministers' Deputies). *European and international standards in the field of justice.* K, 2015. 249–269; Recommendation Rec (2001) 3 of the Committee of Ministers of the Council of Europe to member states on the delivery of court and other legal services to the citizen through the use of new technologies (adopted by the Committee of Ministers on 28 February 2001 on 743 meeting of Ministers' Deputies). *European and international standards in the field of justice.* K, 2015. 270–275; Recommendation Rec (2003) 14 of the Committee of Ministers of the Council of Europe to member states on the interoperability of information systems in the justice sector (adopted by the Committee of Ministers on 9 September 2003 on the 851 meeting of Ministers' Deputies). *European and international standards in the field of justice.* K, 2015. 276–281; Recommendation Rec (2003) 15 of the Committee of Ministers to member states on the provision of information through the media in relation to criminal proceedings (adopted by the Committee of Ministers on 9 September 2003 on the 851 meeting of Ministers' Deputies). *European and international standards in the field of justice.* K, 2015. 282–286.

of justice must be fair and timely, as it is how substantive law is enforced[3].

In our opinion, information technology in civil proceedings should be understood as a systematically organized set of information and communication processes, methods, ways and means of creating, collecting, providing, accumulating, recording, using, storing, processing, generalizing, systematizing and transmitting judicial information in digital form, which ensures openness, accessibility and reliability of information about the activities of courts and their consequences, automating the process of document flow and recording of court proceedings, speeding up the circulation of information in courts, increasing the efficiency of interaction between participants in civil proceedings, which contributes to improving the level of judicial protection, guaranteeing the rights of litigants, increasing confidence in the judiciary and improving public opinion about the courts, creating a positive image of the judicial system in the public consciousness; increase the efficiency of the administration of justice in civil proceedings[4].

The analysis of case law shows that information technology is increasingly being used in the administration of justice in civil cases in Ukraine. At the same time, the courts are trying not only to comply with the provisions of national legislation, but also to adjust their activities in accordance with the standards of a fair trial, taking into account the existing positions of the European Court of Human Rights (hereinafter – the ECHR) on a particular issue. In this regard, in our opinion, within the framework of this study, having summarised the legal positions of the ECHR on compliance with the

[3] CCJE Opinion No. 26 (2023): Moving forward: the use of assistive technology in the judiciary URL: https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7

[4] N. Y. Sakara *Information technologies of civil proceedings and ensuring the right to a fair trial: modern law enforcement practice* in Yu. Prytika and I. Izarova (eds.) *Access to justice in conditions of sustainable development: to the 30th anniversary of Ukraine's independence: Collective monograph*. Kyiv: VD "Dakor", 2021. 381–382

requirements of Article 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter – the ECHR) in the application of certain information technologies, it is advisable to analyse the procedure for establishing modern approaches of national courts, to assess their compliance with the case law of the ECHR and to outline the problems that arise or may arise in this regard.

2. Ensuring the right of access to court by submitting documents in electronic form

The ECtHR considers that where national legislation provides for the possibility of bringing an action and submitting documents to the court in electronic form, the implementation of the right of access to the court in this way cannot be qualified as an abuse of procedural law, even though other methods (such as filing a claim with attachments in paper form) are permitted. Therefore, the refusal of the courts to accept a claim due to the lack of technical equipment for processing information provided in electronic form constitutes a disproportionate restriction of the right of access to court[5]. The ECtHR emphasises that any failures in the operation of telecommunications networks (electronic document management systems, registers), equipment (fax machines, computers, etc.) or other technical problems which may have resulted in applications lodged in due time or annexes thereto not being received by the Court, or being received late, cannot be imputed to a person who has done all that was required of him in order to duly exercise his procedural rights and fulfil his procedural obligations[6]. However, the courts must not be too formal in their approach to the form

[5] *Lawyer Partners A. S. v. Slovakia,* № 54252/07, 3274/08, 3377/08, 3505/08, 3526/08, 3741/08, 3786/08, 3807/08, 3824/08, 15055/08, 29548/08, 29551/08, 29552/08, 29555/08, 29557/08, § 49–56, ECHR 2009, 16 June 2009.

[6] *Tence v. Slovenia,* № 37242/14, § 32–38, 31 May 2016, *Hietsch v. Romania,* № 32015/07, § 20–24, 23 September 2014.

of filing of documents. If there is a mandatory requirement for electronic filing of documents, the courts should still take into account the existence of objective circumstances that make this impossible. For example, if the circumstances of the case make it impossible for a person to fill in the existing electronic form without distorting the information on the case, the courts' refusal to accept documents in paper form leads to a violation of the right of access to court[7].

On 3 October 2017 the Law of Ukraine "On Amendments to the Commercial Procedure Code of Ukraine, the Civil Procedure Code of Ukraine, the Code of Administrative Procedure of Ukraine and Other Legislative Acts" No. 2147-VIII was adopted, which provided for the possibility of applying to the court in electronic form using the Unified Judicial Information and Telecommunication System (hereinafter – UJITS)[8], but its implementation was postponed until the start of the functioning of the this system. As a result, in practice, for some time the courts did not accept as duly filed documents sent in electronic form to the official e-mail address of the court and returned them to the applicant[9]. However, this method was later recognised as admissible if the documents were signed with an electronic digital signature[10], i.e. this procedure was considered as an alternative to filing a lawsuit using the

[7] *Xavier Lucas v. France,* № 15567/2, § 53–59, 09 June 2022.

[8] Law of Ukraine "On Amendments to the Commercial Procedure Code of Ukraine, the Civil Procedure Code of Ukraine, the Code of Administrative Procedure of Ukraine and Other Legislative Acts" of 3 October 2017 № 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147%D0%B0-19#Text

[9] Judgement of the Civil Cassation Court in structure of the Supreme Court of 19 December 2018, case № 226/1204/18 (proceeding № 61-41499св18); Judgement of the Civil Cassation Court in structure of the Supreme Court of 25 March 2019, case № 226/1858/2018-ц (proceeding № 61-45607св18) etc.

[10] Judgement of the Joined Chamber of Civil Cassation Court in structure of the Supreme Court of 05 September 2019, case № 530/1727/16-ц (proceeding № 61-47059сво18); Judgement of the Civil Cassation Court in structure of the Supreme Court of 29 April 2020, case № 530/795/18 (proceeding № 61-47066 св 18) etc.

"Electronic Court" subsystem, which was functioning in test mode in some courts.[11]

Subsequently, the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine in Order to Ensure the Gradual Implementation of the Unified Judicial Information and Telecommunication Syste" No. 1416-IX of 27 July 2021[12] was adopted, and on 17 August 2021 the High Council of Justice approved the Regulation on the Procedure for the Functioning of Certain Subsystems (Modules) of the Unified Judicial Information and Telecommunication System (hereinafter – Regulation on the UJITS)[13]. As a result, three subsystems of the UJITS were officially put into operation on 5 October 2021 – Electronic Cabinet, Electronic Court and Video Conferencing Subsystem.

Despite the fact that at the legislative level the obligation for some persons (lawyers, notaries, private bailiffs, bankruptcy administrators, forensic experts, state authorities, local governments and business entities of the state and municipal sectors of economy) to register in the UJITS and to use only this system for sending documents to the court was envisaged from the very beginning of the implementation of electronic document management in courts, it was not implemented in practice. As a result, two approaches have

[11] On conducting testing of the "Electronic Court" subsystem in local and appellate courts: Order of the State Judicial Administration of Ukraine of 22 December 2018 № 628 URL: https://dsa.court.gov.ua/userfiles/media/628_18.pdf; On the introduction of the "Electronic Court" and "Electronic Cabinet" subsystems into trial operation: Order of the State Judicial Administration of Ukraine dated June 1, 2020 № 247 URL: https://ips.ligazakon.net/document/view/SA20028?ed=2020_06_01&an=19

[12] Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine in Order to Ensure the Gradual Implementation of the Unified Judicial Information and Telecommunication System" No. 1416-IX of 27 July 2021. URL: https://zakon.rada.gov.ua/laws/show/1416-20#Text

[13] Regulation on the Procedure for the Functioning of Certain Subsystems (Modules) of the Unified Judicial Information and Telecommunication System: Decision of the High Council of Justice of 17 August 2021 № 1845/0/15-21 URL: https://zakon.rada.gov.ua/rada/show/v1845910-21

been established in case law as to the admissibility/inadmissibility of submitting an electronic procedural document with an electronic digital signature to the court by sending it to the official e-mail address of the court.

According to the first, the submission of an electronic procedural document to the court by sending it to the official e-mail address of the court is proper and permissible[14], and accordingly the courts accepted such applications and considered them on their merits. The second, on the other hand, stated that such a method of sending documents was not provided for in the applicable procedural legislation[15], and therefore the courts returned applications sent in this way as unsigned by the applicant. The resolution of this procedural issue was referred to the Grand Chamber of the Supreme Court in order to formulate a uniform enforcement practice[16].

The Grand Chamber of the Supreme Court concludes that a distinction should be made between the method of applying to the court and the requirements for the form of a procedural document. If an electronic document is signed with an electronic signature that ensures the identification of a person, but the electronic signature is not applied using the UJITS subsystems, and the procedural document is sent to the official e-mail address

[14] Ruling of the Grand Chamber of the Supreme Court of 28 February 2019, case № 200/12772/18 (proceeding № 14–99 зц 19), Judgement of the Joined Chamber of the Civil Cassation Court in structure of the Supreme Court of 05 September 2019, case № 530/1727/16-ц (proceeding № 61-47059сво18), Judgement of the Civil Cassation Court in structure of the Supreme Court of 10 June 2020, case № 226/1863/2018 (proceeding № 61-45602св18) etc.

[15] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 21 December 2019, case № 910/12245/19, Judgement of the Grand Chamber of the Supreme Court of 10 February 2021, case № 9901/335/20 (proceeding № 11-361заі20), Judgement of the Grand Chamber of the Supreme Court of 01 July 2021, case № 9901/76/21 (proceeding № 11-137заі21), Judgement of the Administration Cassation Court in structure of the Supreme Court of 12 August 2021, case № 200/6370/20-а (proceeding № К/9901/33163/20) etc.

[16] Ruling of the Civil Cassation Court in structure of the Supreme Court of 22 June 2022, case № 204/2321/22 (proceeding № 61-4845св22).

of the court, there are no legal grounds for claiming that such an electronic document is not signed. The opposite approach eliminates the legal force of an electronic document and the presumption that a qualified electronic signature is equivalent to a handwritten signature, it also contradicts Part 1 of Article 8 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" and Article 18 of the Law of Ukraine "On Electronic Trust Services". The requirement to apply to the court through the UJITS subsystems is mandatory for persons specified in clause 10 of the UJITS Regulation and those who have voluntarily registered official e-mail addresses in the UJITS. An application to the court by an individual (other than lawyers and other persons specified in clause 10 of the Regulation on the UJITS) through the official e-mail address of the court with an electronic procedural document signed with an electronic digital signature is a proper and legitimate way of direct application to the court, which is identified with direct application to the court through the office or traditional means of postal communication and should be qualified as a direct application to the court. In view of the "quality of law", an individual (except lawyers and other persons provided for in clause 10 of the Regulation on the UJITS), when applying to the court, must clearly understand that he or she has the possibility to create and send procedural or other documents electronically through the "Electronic Court" subsystem, but registration of an official e-mail address for an individual in the UJITS is voluntary, and a qualified electronic signature has a presumption of conformity with a handwritten signature. Therefore, in this case, applying to the court through the official e-mail address of the court with an electronic procedural document signed with an electronic digital signature is similar to applying directly to the court[17].

[17] Judgement of the Grand Chamber of the Supreme Court of 13 September 2023, case № 204/2321/22 (proceeding № 14-48цс22), para 7.50–7.54, 7.59.

On 29 June 2003 the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on the Mandatory Registration and Use of Electronic Offices in the Unified Judicial Information and Telecommunication System or its Separate Subsystem (Module) Ensuring Document Exchange"[18] No. 3200-IX was adopted, which amended the Civil Procedural Code of Ukraine, the Commercial Code of Ukraine and the Code of Administrative Procedure of Ukraine. Thus, Part 6 of Article 14 of the Civil Procedural Code of Ukraine, as amended, stipulates that lawyers, notaries, public and private bailiffs, insolvency administrators, forensic experts, public authorities and other state bodies, local self-government bodies and other legal entities shall register their electronic accounts in the UJITS or its separate subsystem (module) providing for the exchange of documents on a mandatory basis. Other persons may register their electronic accounts in the UJITS or its separate subsystem (module) providing for the exchange of documents on a voluntary basis. The procedural results provided by this Code in case of an application to the court with a document of a person who is obliged to register an electronic cabinet in accordance with this Part, but has not registered it, shall be applied by the court also in case if the interests of such person are represented by a lawyer in the case. If the registration of an electronic cabinet in the UJITS or its separate subsystem (module) providing for the exchange of documents contradicts the religious beliefs of a person who is obliged to register it in accordance with this Part, the procedural consequences of the appeal of such a person to the court without registering an electronic cabinet shall be to leave his document without movement, to return it or to leave it

[18] The Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on the Mandatory Registration and Use of Electronic Offices in the Unified Judicial Information and Telecommunication System or its Separate Subsystem (Module) Ensuring Document Exchange" No. 3200-IX on 29 June 2003. https://zakon.rada.gov.ua/laws/show/3200-20#Text

without consideration, provided that the person has declared such circumstances simultaneously with the submission of the relevant document by submitting a separate application. However, Part 8 of Article 14 of the Code of Civil Procedure of Ukraine provides that registration in the UJITS or its separate subsystem (module) providing for the exchange of documents does not deprive a person of the right to submit documents to the court in paper form.

At present, it is possible to submit an application to the court in either paper or electronic form. However, the methods of electronic submission of documents are differentiated according to the obligation to register an electronic cabinet in the UJITS and its direct registration. Thus, the procedure common to all entities is the use of the UJITS for the exchange of documents. As an exception, a person who does not have a registered electronic cabinet and who personally applies to the court without using the services of a lawyer, or another person who has technical difficulties in using the UJITS subsystems[19], which are confirmed by appropriate evidence (a printout of the screen of the electronic cabinet page with the generated document in the "referred" status; a letter from the UJITS administrator, etc.)[20], may send documents to the official e-mail address of the court. At the same time, the submission of documents in paper form does not exempt persons who are obliged to register an electronic cabinet from fulfilling this obligation.

Submitting documents to the court in electronic form has certain characteristics.

Firstly, whatever the method of submission and whatever the type of application, such applications are signed by the electronic

[19] Judgement of the Grand Chamber of the Supreme Court of 13 September 2023, case № 204/2321/22 (proceeding № 14-48цс22), para 8.10–8.11.

[20] Judgement of the Administrative Cassation Court in structure of the Supreme Court of 21 March 2023, case № 560/4377/22 (proceeding № К/990/28546/22)

digital signature of the applicant[21], the existence of which must be verified by the court staff using the online service for the creation and verification of qualified and advanced electronic signatures on the official website of the CCA (www.czo.gov.ua)[22]. Moreover, the concepts of "signing with an electronic digital signature" and "verifying an electronic digital signature" are not identical in terms of time, since signing occurs when a person takes action to send documents to the court, and verification occurs later, when a court clerk acts. However, when assessing compliance with the time limits for filing an application with the court, the time of signing documents with an electronic digital signature should be considered[23].

An original document is a document in electronic form and its paper form is a copy of the document reproduced on paper. Therefore, the court is obliged to check the electronic document for signatures, not its paper copy. An error made by the court clerk in producing a paper copy cannot have the procedural consequence of leaving the application without movement or returning it as unsigned, since this is due to the actions (inactions) of the court clerk and does not depend on the actions of the applicant in submitting the application[24]. If the documents are exchanged between the

[21] Judgement of the Civil Cassation Court in structure of the Supreme Court of 26 May 2021, case № 565/195/19 (proceeding № 61-2692св20), Judgement of the Civil Cassation Court in structure of the Supreme Court of 26 April 2022, case № 757/6877/21-ц (proceeding № 61-15898св21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 03 February 2021, case № 295/12247/19 (proceeding № 61-12247св20), Judgement of the Civil Cassation Court in structure of the Supreme Court of 22 April 2020, case № 360/1789/17 (proceeding № 61-1997св19) etc.

[22] Judgement of the Civil Cassation Court in structure of the Supreme Court of 30 November 2022, case № 2–317/11 (proceeding № 61-6880св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 22 March 2023, case № 755/1549/22 (proceeding № 61-6415св22).

[23] Judgement of the Civil Cassation Court in structure of the Supreme Court of 09 June 2021, case № 755/10972/19 (proceeding 61-6483св21)

[24] Judgement of the Administration Cassation Court in structure of the Supreme Court of 08 June 2023, case № 466/566/22 (proceeding № К/990/25689/22)

applicant and the court via the official e-mail of the court, the court clerk are obliged to check the e-mail at least twice a day and to submit the documents for registration in due time. Failure to comply with the rules of registration and acceptance of electronic correspondence in courts results in the impossibility of imposing on the applicant the obligation to prove the circumstances of the proper submission of applications to the court[25].

Secondly, all the annexes attached to the application are in electronic form and constitute either electronic evidence or electronic copies of written evidence, which, despite their similarity in form, are different from each other. Thus, the main characteristic of electronic evidence is the absence of a strict link to a specific material source. The same electronic document (video recording) may exist on different media. All copies of electronic evidence that are identical in content can be considered as originals, differing only in the time and date of their creation[26]. If scanned or photographed copies of written evidence are attached to the application, they are electronic copies and must be certified by an electronic digital signature. Otherwise, such evidence should be declared inadmissible, and the court may not take it into account in the course of the proceedings[27].

Thirdly, the court fee for filing such applications is paid with a reduction coefficient, even though not all subsystems of UJITS have been launched[28]. At the same time, the court fee can be paid either

[25] Judgement of the Civil Cassation Court in structure of the Supreme Court of 07 December 2022, case № 522/7002/17 (proceeding № 61-10558св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 07 December 2022, case № 709/3/22 (proceeding № 61-9192св22)

[26] Judgement of the Criminal Cassation Court in structure of the Supreme Court of 10 September 2020, case № 751/6069/19 (proceeding № 51-1704км20)

[27] Judgement of the Civil Cassation Court in structure of the Supreme Court of 07 February 2024, case № 712/8019/18(proceeding № 61-9112св23)

[28] Judgement of the Grand Chamber of the Supreme Court of 16 November 2022, case № 916/228/22 (proceeding № 12-26гс22).

online in the client's bank account that meets the requirements of the Law of Ukraine "On Court Fee", and the receipt sent to the e-mail address as a confirmation of payment of the court fee is the only possible document to confirm the payment of the court fee online and has evidentiary force to meet its requirements[29], or, as provided in paragraph 44 of the Regulation on UJITS, through the Electronic Court online when the relevant document is being created. In this case, the information will be automatically added to the document being drawn up.

Fourthly, a person is exempted from the obligation to attach copies of the application with attachments in accordance with the number of participants in the case[30], as required by para 1 part 1 of Article 177 of the Civil Procedure Code of Ukraine. Instead, the party must prove that it has sent a copy of the documents submitted to the court by letter with a description of the attachment to other parties to the case. If the other party of the case has a registered electronic cabinet in accordance with the entered identification data, the E-Court functionality automatically provides the court and the party to the case with proof of sending documents submitted to the court to the electronic cabinets of other parties to the case, which relieves them of the obligation to send documents in paper form. Similarly, if another party to the case was obliged to register an electronic cabinet in the UJITS but failed to do so, that party is relieved of that obligation. However, a printout of e-mail correspondence regarding the sending of a copy of the application to the other party to the case is not an appropriate proof of the fulfilment of this obligation, as it does not allow the court to verify the validity of such sending, as well

[29] Judgement of the Civil Cassation Court in structure of the Supreme Court of 27 January 2021, case № 754/9573/13-ц (proceeding № 754/9573/13-ц)

[30] Judgement of the Civil Cassation Court in structure of the Supreme Court of 14 February 2024, case № 753/11499/23 (proceeding № 61-17227св23)

as to check which document was sent to the party to the case and to establish the fact of receipt of such correspondence[31]. Sending copies to an e-mail address (which does not have the status of an official address) to other parties to the case is an additional way of informing the court of the appeal, but is not an alternative[32]. This approach cannot be interpreted as a manifestation of excessive formalism, since the ECHR in its decisions assumes that the procedure established by procedural law cannot be changed at will, but only at the discretion of the parties to the case[33].

Fifthly, in order to confirm the representative's authority, either an electronic power of attorney, an electronic warrant, or scanned copies of a power of attorney or a lawyer's warrant originally issued in paper form may be submitted. In this case, an electronic power of attorney is generated in the eCourt subsystem if the relevant principal and his/her representative have personal electronic accounts, which implies that these persons have an electronic digital signature. An electronic power of attorney shall only be issued if it is signed with the electronic key of the principal using the algorithms of the subsystem. Subsequently, such an electronic power of attorney is automatically attached to the application submitted by the representative on behalf of the principal through the Electronic Court subsystem, but users do not have the possibility to influence its content and appearance in any way, i.e. it is independently generated by the subsystem in accordance with the selected scope of the representative's powers. In the case of the creation of an electronic power of attorney using the "Electronic Court" subsystem, a person does not need to provide an additional paper copy of such power of

[31] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 04 October 2022, case № 910/622/22

[32] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 08 May 2023, case № 911/2003/22

[33] *C. N. c. Luxembourg,* № 59649/18, § 53, 12 October 2021.

attorney or any other document confirming the representative's powers[34]. Such authorizations are automatically attached to applications when they are submitted, i.e. a person who submits an application to the court using the "Electronic Court" subsystem has a legitimate expectation that the court will receive the documents sent together with the electronic authorization without hindrance[35].

In our view, the innovations introduced regarding the electronic filing of court cases by the parties are positive. The jurisprudence is as far as possible adapted to modern trends and in most cases takes into account the existing standards of access to court. However, there are a number of problems with which the judicial system is confronted. The first is a purely technical one, related to the unstable operation of the UJITS subsystems, aggravated by power cuts and the lack of internet in some regions of Ukraine. Secondly, the obligation of a party to a case to send paper copies of documents to other parties to the case by registered mail in the case of filing a case in electronic form, provided that other parties to the case do not have, and are not required to have, a registered electronic cabinet, is complicated by the fact that such documents are generated only at the time they are sent to the UJITS. Thirdly, despite all this, in most cases the case files are still generated in paper form, which entails additional costs for the judicial system.

[34] Judgement of the Civil Cassation Court in structure of the Supreme Court of 08 September 2021, case № 486/259/21 (proceeding № 61-9466св21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 25 January 2023, case № 235/8501/21 (proceeding № 61-11615св22), Judgement of the Administration Cassation Court in structure of the Supreme Court of 10 February 2022, case № 560/11791/21 (proceeding № К/9901/43626/21), Judgement of the Administrative Cassation Court in structure of the Supreme Court of 30 March 2023, case № 580/140/23 (proceeding № К/990/4464/23) etc.

[35] Judgement of the Administrative Cassation Court in structure of the Supreme Court of 23 August 2023, case № 352/732/22 (proceeding № К/990/3946/23).

3. Respect for fair trial guarantees and the use of certain information technologies to inform the litigants

Among the fair trial guarantees highlighted by the ECtHR that are somehow related to the use of information technology, one can single out the proper notification of the time and place of the trial.

The ECtHR considers that, although Article 6 ECHR does not lay down any requirements as to the specific form in which procedural documents should be served, the general concept of a fair trial, which includes the fundamental right to a fair hearing, requires that every person should be informed of the proceedings which affect his or her rights, freedoms, and interests. At the same time, the right of access to the courts under Article 6(1) of the ECHR provides for the right to be duly notified of decisions, which is of particular importance where the possibility to appeal against them is limited to a certain period[36]. The fact that an applicant may not receive correspondence from the court is not itself sufficient to establish that his rights have been violated. In this regard, the ECtHR takes into account whether the documents were sent in the manner prescribed by the applicable law, as well as the behavior of the applicant, who, being aware of the existence of judicial proceedings against him, remains passive and does not take any measures to ensure that the correspondence sent to him is received[37].

The ECHR allows for notification of the parties to the case via the Internet, in particular by posting a notice on a specific website. However, such notification will be considered proper if the information provided in this way is predictable by the way enshrined in law, consistent, accessible to a large number of persons and understandable, i.e. it provides a person with an

[36] *Šild v. Slovenia* (dec.), № 59284/08, § 30, 17 September 2013

[37] *Sydorenko v. Ukraine (dec.),* № 73193/12, 18 February 2021

opportunity to find out about a decision that may potentially affect his or her rights. At the same time, considering the principle of proportionality, courts should also take into account the circumstances of the case, which may indicate a lack of access to a computer or the Internet, computer illiteracy and other factors that may have prevented access to the requested decision[38]. In analyzing the notification of the defendant by means of a public announcement in the press, the ECtHR pointed out that national courts should exercise due diligence when using this method of notification, particularly in cases involving a sensitive area of legal relations, by taking an active position and taking additional measures to verify and find out the location of the defendants by contacting the relevant law enforcement authorities, and by imposing on the claimant the obligation to provide additional evidence in support of the claim[39].

The procedure for notifying the parties of the time and place of the hearing has recently undergone some formal changes. Thus, in accordance with para 1, part 6 of Article 128 of the Civil Procedure Code of Ukraine in the version in force until 18 October 2023, In accordance with the provisions of this Code, notifications and copies of pertinent documentation were transmitted to the official email address of the relevant litigant, in the event that such an address was available, or alternatively, by registered mail with acknowledgment of receipt in the absence of an email address. If the addressee was a party to the case, notifications were delivered by courier to the address provided by that party. In this case, the official email address was deemed to be the email address provided by the user in the UJITS or the email address listed in one of the official registers (clause 5.8 of the Regulation on the UJITS). The

[38] *Stichting Landgoes Steenbergen and Others v. Netherlands,* no. 19732/17, § 47–54, 16 February 2021.

[39] *Gakharia v. Georgia,* № 30459/13, § 39–44, 17 January 2017.

court practice has established that such an address comprises an identifier, an "@" sign and a domain name. The identifier for legal entities was the identification code of the legal entity, while for individuals and individual entrepreneurs it was the identification number of the individual taxpayer (in the absence of an identification number – the series and number of the citizen's passport). The domain name was the name in the domain "mail.gov.ua")[40]. As the official email address was the service of the Electronic Cabinet, the procedural terms commenced on the following day after the documents were delivered to the Electronic Cabinet in the "My Cases" section[41]. This was the moment at which the procedural document was delivered to the litigant in electronic form. This position, although implemented in court practice, did not fully comply with the legislation in force at the time. A person could specify any email address when registering with the UJITS, which, upon its indication, should be considered as officially registered. This allowed litigants to abuse their procedural rights by referring to the failure to receive court documents in accordance with the procedure established by the current legislation.

The enactment of the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Mandatory Registration and Use of Electronic Offices in the Unified Judicial Information and Telecommunication System or its Separate Subsystem (Module) Enabling Document Exchange" № 3200-IX dated 29 June 2023, which amended the terminology of procedural legislation and the

[40] Judgement of the Civil Cassation Court in structure of the Supreme Court of 01 June 2022, case № 761/42977/19 (proceeding № 61-1933св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 10 February 2022, case № 359/5063/21 (proceeding № 61-21505св21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 27 October 2021, case № 279/5407/20 (proceeding № 61-8744св21) etc.

[41] Judgement of the Supreme Court of 18 April 2020, case № 750/3275/21 (proceeding № 61-21072св21); Judgement of the Supreme Court of 05 April 2023, case № 761/14537/15-ц (proceeding № 61-11084св22).

Regulation on the UJITS, also replaced the term “Official Email Address” with “Electronic Office”. This change aligns with the current version of para 1 part 6 of Article 128 of the Civil Procedure Code of Ukraine, which stipulates that summonses shall be sent to the electronic cabinet of the relevant party to the case.

It is evident that not all participants of civil procedural legal relations are required to register in the UJITS and, accordingly, have an official email address and an electronic cabinet. However, they must be notified of the time and place of the case. This has prompted the court practice to consider the possibility of sending court summonses and court decisions to email, even though this is not an official method of communication. Instead, it is indicated by the party to the case in the documents submitted to the court as a means of communication.

Initially, the courts adopted a formal approach to the application of procedural law, taking the legal position that such notification could not be considered proper[42]. However, over time, this approach has changed, influenced by number of objective circumstances, including underfunding of the judicial system. In addition, the behavior of the party to the case has also been taken into account when deciding whether the notification is proper. Consequently, if the litigant had indicated their personal email address as the official one in the statements sent to the court and had sent documents from it at the request of the court, then in the event of sending a summons or a court decision to this email address, the litigant was considered to have been duly notified.[43]. This legal position was subsequently developed in further case law and transformed into the “presumption of awareness”. According

[42] Judgement of the Civil Cassation Court in structure of the Supreme Court of 01 June 2020, case № 761/42977/19 (proceeding № 61-1933св22).

[43] Judgement of the Civil Cassation Court in structure of the Supreme Court of 13 July 2022, case № 761/14537/15-ц (proceeding № 61-3069св21).

to this, courts should assume that if a party has provided the court with an email address (although it may not have done so) by indicating it in a claim (application), it should be assumed that the party wishes, or at least does not object, to have these means of communication used by the court. This, in turn, imposes an obligation on the litigant to receive and respond to notifications. In view of this, a court that communicates with a party through the means communicated by him or her acts lawfully and in good faith. Therefore, one should proceed from the "presumption of awareness": the person to whom the court's notice is addressed through such means of communication knows or at least should have known about the notice[44]. Moreover, in the context of martial law, the sending of court decisions to the e-mail address indicated by the litigant in the documents submitted by him/her as his/her own e-mail address is appropriate and aimed at achieving the goal of notifying the litigant about the court decision[45].

Nevertheless, not all judges, including those of the Supreme Court, share the possibility of applying the "presumption of awareness", so this issue was referred to the Grand Chamber of the Supreme Court. The latter came to the conclusion that the procedural law provides for two ways of sending a court decision – by sending a registered letter with acknowledgement of receipt and electronically – through the "Electronic Cabinet", including by sending a letter to the official e-mail via the UJITS subsystems in cases provided for in para 37 of Chapter 2 of Section III of the Regulation on the UJITS. Sending a court decision in one way or

[44] Judgement of the Civil Cassation Court in structure of the Supreme Court of 27 April 2023, case № 727/474/16-ц (proceeding № 61-8157св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 26 April 2023, case № 127/32270/21 (proceeding № 61-12567св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 20 January 2023, case № 465/6147/18 (proceeding № 61-8101св22) etc.

[45] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 28 April 2023, case № 904/272/22.

another to a party of the case is a procedural obligation of the court. The desire of a party (individual) to indicate his/her personal email address in the claim (application) only indicates the person's desire to receive correspondence from the court by an additional means of communication and does not relieve the court of the obligation to comply with the requirements of the law, in particular, to send the court decision in accordance with the procedure provided for in Article 272 of the Civil Procedure Code of Ukraine (as amended at the time of the decision by the court of first instance). Sending the relevant procedural documents to the email address of the party to the case specified in the documents submitted to the court is not prohibited and may be carried out as an additional one, but such actions cannot replace the proper sending of the court decision to the party in accordance with Article 272 of the Code of Civil Procedure of Ukraine (as amended at the time of the decision of the court of first instance)[46].

However, in our opinion, the use of such a construction is permissible in modern realities, even considering the practice of the ECHR, and does not lead to a violation of the right to a fair trial.

First of all, its emergence is primarily due to objective circumstances that the legislator could not have foreseen when introducing the notification of the litigants using the electronic cabinet services. These include, of course, the introduction of martial law and the ongoing armed conflict in Ukraine, which makes it impossible to send registered letters of notification by post. However, as noted above, individuals are not required to register electronic accounts with the UJITS. Many individuals have changed their actual location, including by leaving Ukraine, and as a result, information in the demographic register does not always

[46] Judgement of the Grand Chamber of the Supreme Court of 10 April 2024, case № 454/1883/22 (proceeding № 14-117цс23).

reflect the actual data. However, para 4, part 8 of Article 128 of the Civil Procedure Code of Ukraine establishes a "legal fiction" that the day of service of a court summons is the day on which a notice of absence of a person at the address of the person's location, place of residence or stay registered in accordance with the procedure established by law is made in the postal notification, although in practice such a person remains unnotified.

Secondly, the legal basis for qualification of the e-mail message specified by the litigant as proper remains, to some extent, clause 120 of the Regulation on UJITS, which provides that prior to the start of operation of all subsystems (modules) of the UJITS, the court shall send case documents to persons, other than persons who are obliged to register their Electronic Offices in the UJITS or who have registered Electronic Offices in the UJITS, to the e-mail address from which the court received documents certified with a qualified electronic signature. If the court sends documents to the e-mail address from which the court received documents certified with a qualified electronic signature, the risks of technical impossibility to deliver the court document to the relevant address of the litigant are the responsibility of the litigant.

Thirdly, the ECHR has repeatedly emphasized that the parties to a case must show due diligence and be interested in the outcomes of the case. In this respect, if a party provides the court with his/her e-mail address, he/she should be aware that the latter may be used by the court as a means of communication, since the current procedural legislation does not lay down any additional conditions for this. At the same time, such an address must be provided by the party itself, and not by the opposing party.

In addition to the use of e-mail, the current legislation also provides for the possibility of notifying the parties to the case by publishing an announcement on the official website of the

judiciary. However, the legality of using this method of notification is assessed on the basis the territorial criterion and the criterion of the legal status of the person.

In accordance with the territorial criterion of Article 12–1 of the Law of Ukraine "On Ensuring the Rights and Freedoms of Citizens and the Legal Regime in the Temporarily Occupied Territory of Ukraine"[47] if the last known address of the residence (stay), location or place of work of the litigants is located in the temporarily occupied territory, the court shall summon or notify the litigant, who does not have an electronic cabinet, about the date, time and place of the first court hearing in the case through an announcement on the official web portal of the judiciary of Ukraine. It must be published no later than twenty days before the date of the court hearing. The litigants should be informed in the same way about the date, time and place of other court hearings or procedural actions, but the announcement should be published no later than ten days before the date of such court hearing or procedural action. The publication of such notice shall constitute notice to the defendant of the date, time, and place of the hearing. The litigants, whose last known address of residence (stay) or location is in the temporarily occupied territory and who do not have an electronic cabinet, shall be notified about the court decision by posting information on the official web portal of the judiciary of Ukraine with a link to the web address of such court decision in the Unified State Register of Court Decisions or by posting the text of the relevant court decision on the official web portal of the Judiciary of Ukraine, taking into account the requirements of the Law of Ukraine "On Access to Court Decisions", if access

[47] Law of Ukraine "On Ensuring the Rights and Freedoms of Citizens and the Legal Regime in the Temporarily Occupied Territory of Ukraine" of 20 October 2014 № 1706-VII. URL: https://zakon.rada.gov.ua/laws/show/1207-18

to the Unified State Register of Court Decisions is restricted. From the moment such information is published, the person shall be deemed to have received the court decision. The procedure of summoning to a court and notification of a court decision provided for in this Article may be applied to other litigants whose place of residence is located in the territory of Ukraine.

Part 11 of Article 128 of the Civil Procedure Code of Ukraine also provides that, depending on the criterion of the legal status of the case, the litigants may be notified by publication of an announcement on the official website. The defendant, a third party, a witness whose registered place of residence (stay), location or place of work is unknown, as well as an interested person in cases of issuing a restraining order, are summoned to court by an announcement on the official website of the judicial system of Ukraine, which must be published no later than 10 days, and in the case of issuing a restraining order – no later than 24 hours before the date of the relevant court hearing. Publication of the summons shall be deemed to notify the person of the date, time and place of the hearing. The use of this method of notification should always be preceded by clarification of the place of residence of such persons[48]. At the same time, this method will not be recognized as appropriate if the case file contains information about the registered residence of such litigants[49] or if the claimant

[48] Judgement of the Civil Cassation Court in structure of the Supreme Court of 22 February 2024, case № 638/16162/19 (proceeding № 61-14851св23), Judgement of the Civil Cassation Court in structure of the Supreme Court of 23 November 2023, case № 201/6810/19 (proceeding № 61-6680св22) etc.

[49] Judgement of the Civil Cassation Court in structure of the Supreme Court of 11 November 2022, case № 0417/2–4308/2011 (proceeding № 61-12162св21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 05 October 2022, case № 757/72370/17 (proceeding № 61-17265св20), Judgement of the Civil Cassation Court in structure of the Supreme Court of 10 August 2022, case № 757/28189/20-ц (proceeding № 61-6264св22) etc.

is notified by means of such information[50]. Exceptionally, if the court has summoned a person to appear in court by placing an announcement on the official website of the judiciary, but such a person later – when appealing against court decisions – admits that he or she does not live at any of the addresses available to the court, but one of them is the person's officially registered address (indicating the address of residence the address which was not and could not be known to the other litigants or the court), the use of such a method of notification may be recognized as permissible and the only possible way of informing the person of the time and place of the hearing[51].

However, the courts should be aware that this method of notification is by nature a "legal fiction" which can be disproved at the request of a person who provides irrefutable evidence to prove that he or she was not and could not have been notified in this way, which is in line with the practice of the ECtHR. However, the annulment of court decisions for failure to properly notify one of the litigants should take place after the assessment of such notification, considering the content of the principles of proportionality and legal certainty, as well as the fact that a correct court decision on terms of the merits cannot be annulled on formal grounds alone. In our view, several issues should be considered. First, the procedural status of such a litigant is of great importance. For example, if a person is a third party who has no independent claims in relation to the subject-matter of the dispute, the court should take into account that the court judgement does not resolve the issue of the rights and obligations of such person, since its procedural status provides only for a possible effect on its

[50] Judgement of the Civil Cassation Court in structure of the Supreme Court of 13 September 2022, case № 554/2176/20 (proceeding № 61-16111св21).

[51] Judgement of the Civil Cassation Court in structure of the Supreme Court of 09 August 2023, case № 158/3041/21 (proceeding № 61-3363св23).

rights and obligations, and the court judgment cannot be based on the assumption of a further violation of the rights of such a person. Secondly, the time elapsed between the entry into force of the judgment and the lodging of the appeal, which directly affects compliance with the principle of legal certainty should be mentioned. Thirdly, the arguments put forward by the person appealing against the court decision in question are important, i.e. whether they are purely procedural in nature or whether they also relate to incorrect determination of the circumstances of the case or application of substantive law, i.e. whether a court judgment of the opposite content may be rendered. The annulment of a judicial decision for the sake of annulment, without the possibility of further alteration of its content, may be qualified as legal purism, which, like the failure to notify a party to the case, results in a violation of the right to a fair trial[52].

According to part 9 Article 128 of the Civil Procedure Code of Ukraine the court may summon or notify a witness, expert, translator, specialist, and in cases of urgent need provided for by this Code, in particular in cases of issuance of a restraining order, also the parties to the case by telephone, telegram, fax, e-mail or message by other means of communication (including mobile) that ensures the recording of the message or summons. However, this provision has a limited scope in terms of the persons who may be notified in this way: as a rule, notification of the parties to the case, other than the parties in cases on the issuance of a restraining order, in the following ways is recognized as not complying with the established procedure for notification of the date, time and place of the case[53].

[52] Judgement of the Civil Cassation Court in structure of the Supreme Court of 06 March 2024, case № 359/11910/14-ц (proceeding № 61-15022св23).

[53] Judgement of the Civil Cassation Court in structure of the Supreme Court of 12 April 2023, case № 127/18576/21 (proceeding № 61-12428св22), Judgement of the Civil

Pursuant to Part 13 of Article 128 of the Civil Procedural Code of Ukraine, notification of the assignment of a case for consideration and of the date, time and place of a court hearing or relevant procedural action shall be provided by means of mobile communications that ensure the fixation of a message or call by sending text messages to such a party to the case indicating the web address of the relevant decision in the Unified State Register of Court Decisions in the manner prescribed by the Regulations on UJITS. The absence of such an indication makes it impossible to use this method[54].

With the adoption of the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Mandatory Registration and Use of Electronic Cabinets in the Unified Judicial Information and Telecommunication System or its Separate Subsystem (Module) Ensuring Document Exchange" No. 3200-IX dated 23 June2023, the form in which court decisions are sent to the case file has undergone some changes. Thus, in accordance with para 1 part 7 of Article 14 of the Civil Procedure Code of Ukraine, a person who has registered an electronic cabinet in the UJITS or its separate subsystem (module), providing for the exchange of documents, the court shall serve any documents in cases in which such a person participates exclusively in electronic form by sending them to the electronic cabinet of such a person, which does not deprive him/her of the right to receive a copy

Cassation Court in structure of the Supreme Court of 07 December 2022, case № 520/5811/13 (61-1248св21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 31 August 2021, case № 463/8859/20 (proceeding № 6106211св22) etc.

[54] Judgement of the Civil Cassation Court in structure of the Supreme Court of 08 May 2023, case № 201/9898/19 (proceeding № 61-12531св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 31 January 2023, case № 693/812/21 (proceeding № 61-11611св22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 10 November 2022, case № 440/222/19 (proceeding № 61-8993св22) etc.

of the court decision in paper form upon a separate application. Thus, persons who are obliged to register an electronic cabinet in the UJITS or who have registered it on their own initiative, will be notified of the court decision, including its content, only in electronic form by sending it to the Electronic Cabinet, which does not deprive them of the right to receive a paper copy upon a separate request, while individuals will be sent paper copies of court decisions.

4. The right to an adversarial procedure and access to electronic case files

The ECtHR has assessed the compliance with the right to a fair trial in cases where applicants complained about the impossibility of getting acquainted with the case file available in electronic form. In such cases, the ECtHR draws attention to several circumstances: whether the person was given the opportunity to access such materials at all, and whether he or she made proper use of it. Thus, there is no violation of the right under Article 6(1) of the ECHR if access was granted but the person could only study the material in its entirety with the aid of special reading programmes which were not freely available but could only be used in the premises of a particular state body under the supervision of its employees, or if the person had partial access to electronic files but could not study them all because he had chosen an ineffective method of familiarizing himself with the material[55]. Similarly, where a person has not made a request for access, but this procedural step is mandatory, the inability to familiarize himself with the electronic material does not indicate a violation of the right to a fair trial[56]. However, if certain case materials, to which the court refers in its decision are available in electronic form, and the opposing party,

[55] *Rook v. Germany,* № 1586/15, § 60–75, 25 July 2019.

[56] *Sigurdur Einarsson and Others v. Iceland,* № 39757/15, § 92, 4 June 2019.

due to the lack of a certain status (lawyer), does not have access to the judicial system of electronic services and cannot automatically receive information about the receipt of new documents, the foregoing results in a violation of the principle of equality and the right to an adversarial process[57].

An analysis of the cases submitted to the Supreme Court shows that their existence in electronic form is not yet widespread; in most cases, they still exist in paper form. At the same time, the procedure for submitting statements and evidence to the court provides for copies to be given to the opposing party, which minimizes situations in which a person is unaware of their content.

At the same time, the Regulation on UJITS provides that document sent by one of the litigants to a court or other body or institution of the judicial system using the Electronic Court, in cases provided for by law, shall be automatically sent to the Electronic Cabinets of other parties to the case or their attorneys after registration of these documents in the ACDS or automated workflow systems. Information, including information on the receipt and registration of documents in the case, as well as other information leading to a change in the status of the case, shall be sent to the Electronic Cabinet. Persons who do not have registered Electronic Cabinets may, in the cases provided for in this clause, receive documents through the UJITS subsystems to the e-mail address provided by such persons when submitting documents to the court. The UJITS tools shall automatically check whether the person has a registered Electronic Cabinet. If the person has an Electronic Cabinet, the UJITS tools ensure that a confirmation of delivery of the document in the case to the user's Electronic Cabinet is sent to the automated workflow system. Otherwise, the automated workflow system shall receive a notification that the

[57] *Andersen v. Latvia,* № 79441/17, §95–98, 19 September 2019.

person does not have a registered Electronic Cabinet. Documents in the case are sent to the Electronic Case Management System only if the user's (participant's) identification data entered in the automated case management system are available. If the user sends documents in the case using his own Electronic Cabinet, the user's identification data will be automatically entered into the automated workflow system. If a person submits documents in a case in paper form, his/her identification data shall be entered into the automated case management system by a court employee in a mandatory manner. If the submitted documents do not contain the identification data of a party to the case, such data must be entered by a court clerk immediately upon receipt by the court, including at the request of the litigants (para 37, 42–43).

There is currently no case law suggesting that national courts may violate the right to a fair trial by restricting access to electronic case files. However, courts should take into account that according to Article 43(1)(1) of the Civil Procedure Code of Ukraine, the parties to the case have the right to familiarize themselves with the case file, regardless of the form in which it exists, so that such access should be granted in the case of duly executed requests.

5. The right to a public hearing and participation in a court hearing via videoconference

The ECtHR considers that the participation of the parties in a court hearing via videoconference does not in itself contradict Article 6(1) of the ECHR, since it allows for the principle of procedural equality of the parties in cases where it is impossible for a person to appear in court, but the use of this measure must in each case pursue a legitimate aim in order to ensure that the procedure for the presentation of evidence meets the requirements of due process[58].

[58] *Marchello Viola v. Italy,* № 45106/04, § 67, 05 October 2006.

Until recently, the cases before the ECtHR, in which the national courts conducted proceedings by videoconference and examined compliance with the requirements of Article 6(1) of the ECHR, were characterized by the fact that one of the parties was a person sentenced to imprisonment, which prevented him from appearing in court. The ECtHR reasoned that, firstly, videoconferencing can be used both with or without the consent of the parties to the case, but that this must always be motivated. Secondly, effective participation in court proceedings includes not only the right to be present, to hear and to see the parties to the proceedings, but also the right to follow the proceedings without technical difficulties. Thirdly, participation in a court hearing via videoconferencing obliges the court, when dealing with criminal cases on its own initiative, to ascertain whether a person has waived the right to counsel and, if not, to appoint counsel even if the person does not request it, and to provide the accused with effective legal assistance by counsel. This requirement does not generally apply to civil proceedings, which are not characterized by the mandatory participation of a representative. The only exceptions are cases involving legal representatives acting in the interests of incapacitated or partially incapacitated persons and minors. Fourthly, one of the guarantees of a fair trial is the right of the accused and his defense counsel to confidential communication, i.e. the possibility of communicating outside the hearing of third parties. It is considered that in cases where the party to the proceedings and his representative are located in different places, this requirement should be respected in order to ensure the principle of procedural equality of the parties and competition[59].

[59] N. Y. Sakara *The use of information technologies in civil proceedings and compliance with the guarantees of a fair trial: certain aspects* in *Actual problems of protection of informational rights of a person in the conditions of technological challenges and digital reality: materials of the international science and practice conference* (Kyiv, September 17–18. 2019). Kherson, 2019. 42–43.

At the same time, the situation has changed to some extent because of the spread of the coronavirus and the introduction of quarantine restrictions in various countries, which have altered the ability of the parties to the case to attend court hearings in person. At present, the ECtHR does not find a violation of Article 6(1) ECHR on the sole ground that national authorities have restricted the applicant's right to be present in person in a courtroom in civil cases where he or she could participate by videoconference[60].

Pursuant to part 1–3 of Article 212 of the Civil Procedure Code of Ukraine, litigants have the right to participate in a court hearing via videoconference outside the courtroom, provided that the court has the appropriate technical facilities, which shall be specified by the court in the ruling on the opening of the proceedings, unless the court recognizes the presence of such litigant at the court hearing as mandatory. The litigant shall submit a motion to participate in the hearing via videoconferencing outside the courtroom within the same time limit. A copy of the motion shall be sent to the other parties to the case within the same period. The parties to the case shall participate in the hearing by videoconference outside the courtroom using their own technical means and means of electronic identification with a high level of trust in accordance with the requirements of the Laws of Ukraine "On Electronic Documents and Electronic Document Management" and "On Electronic Identification and Electronic Trust Services", in accordance with the procedure established by the Regulations on the UJITS and/or the rules determining the procedure for the operation of its individual subsystems (modules).

It is clear from the above provision that holding a court hearing via videoconference is not only the right of the participant, but also the right of the court[61]. This right of the court cannot be interpreted

[60] *Jallow v. Norway,* № 36516/19, § 59–70.

[61] Judgement of the Civil Cassation Court in structure of the Supreme Court of 31 January 2023, case № 906/943/18.

as unlimited but is a manifestation of discretionary powers. Thus, when scheduling an oral hearing of a case, the court is obliged to ensure the right of the parties to the case to participate in court hearings, which is an element of publicity and openness of the trial as one of the main principles of the judicial process. At the same time, a component of ensuring this right is the participation of a party to the case in a court hearing via videoconference outside the court room. Since participation in a court hearing via videoconference is also the right of the parties to the case, the court may refuse to grant the motion of a party to the case only in cases provided for by law, i.e. if the court does not have the necessary technical facilities or if the appearance of that party at the court hearing is recognized by the court as mandatory[62]. In case the motion to participate in the court hearing via videoconference is granted in accordance with para 7 part 3 of Article 2 of the Civil Procedure Code of Ukraine, the mentioned decision is binding. Thus, the court that issued such a court decision cannot ignore the mandatory nature of its execution. Therefore, the withdrawal of the case from consideration on the appointed date does not mean that the motion is canceled. If the relevant participant has not filed a new motion regarding the procedure for his participation in the proceedings, which cancels his previous motion to participate by videoconference, the appointment of the case withdrawn from consideration on a new date provides for the participation of the relevant participant in the case by videoconference[63].

Only a person with the procedural status of a participant of the case has the right to file a motion for participation in a court hearing via videoconference, which he or she may be lodged no later than five days before the day of the court hearing by filing

[62] Judgement of the Civil Cassation Court in structure of the Supreme Court of 09 August 2023, case № 161/10117/21 (proceeding № 61-3239св22).

[63] Judgement of the Civil Cassation Court in structure of the Supreme Court of 16 August 2023, case № 753/19205/21 (proceeding № 61-7320св22).

a motion for participation in a court hearing via videoconference in any form, i.e. either by setting out the motion in the first statement on the merits of the case or by making it in the form of a motion on a procedural issue and sending a copy to other participants in the case[64]. Such a request may be of a one-time nature, i.e., contain a request to participate in a court hearing via videoconference only in one specific court hearing, or apply to all court hearings[65]. Violation of the deadlines for filing such motion is one of the grounds for refusing to satisfy it and leaving it without consideration[66]. However, in any case, the court must consider such motion before the day of the trial, unless the motion is filed on that day[67] and notify the relevant participant of the results, since both the failure to consider such motion and the failure to notify the participant in time of the consideration of the case without the use of videoconferencing actually leads to a violation of the procedure for proper notification of the time and place of the case[68]. Thus,

[64] Ruling of the Grand Chamber of the Supreme Court of 13 July 2022, case № 910/5201/19 (proceeding № 12-37гс21), Judgement of the Civil Cassation Court in structure of the Supreme Court of 09 June 2021, case № 521/14321/19 (proceeding № 61-11753св20).

[65] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 23 March 2023, case № 905/2371/21.

[66] Judgement of the Civil Cassation Court in structure of the Supreme Court of 27 May 2021, case № 752/17491/17 (proceeding № 61-161св19), Judgement of the Civil Cassation Court in structure of the Supreme Court of 20 March 2020, case № 184/1401/16-ц (proceeding № 61-6167св18), Judgement of the Commercial Cassation Court in structure of the Supreme Court of 14 July 2021, case № 910/11884/19.

[67] Judgement of the Administrative Cassation Court in structure of the Supreme Court of 27 July 2022, case № 580/1802/20 (proceeding № К/990/8511/22), Judgement of the Civil Cassation Court in structure of the Supreme Court of 22 February 2023, case № 466/4418/21 (proceeding № 61-763св23)

[68] Judgement of the Civil Cassation Court in structure of the Supreme Court of 08 March 2023, case № 398/2365/17 (proceeding № 61-12194св22), Judgement of the Commercial Cassation Court in structure of the Supreme Court of 23 February 2022, case № 904/5816/20, Judgement of the Administrative Cassation Court in structure of the Supreme Court of 09 December 2020, case № 675/1175/17 (proceeding № К/9901/50648/18, К/9901/50827/18), Judgement of the Commercial Cassation Court in structure of the Supreme Court of 26 September 2023, case № 922/1163/22.

failure to deliver a copy of the application for satisfaction of the motion to participate in the court hearing via videoconference is a ground for further postponement of the case, since the case file will not contain information on the service of the summons and, accordingly, the party to the case will be considered not properly notified of the time and place of the hearing[69].

Conducting a court hearing via videoconference involves certain risks for the litigants, the consequences of which are shared among them. Thus, when submitting a motion for participation in a court hearing via videoconference, a participant or his/her representative must be aware of the consequences that he/she or the person he/she represents may incur if he/she is unable to participate in a court hearing via videoconference using his/her own technical means[70] or fails to appear in the court designated by him or her in the relevant application[71]. At the same time, connection using own technical means is possible using only the video conferencing subsystem in UJITS and cannot be made using other services, for example, in telephone mode[72]. When satisfying such motion, the court must take into account whether the party to the case requests to allow him/her to participate in the court hearing via videoconference either outside the courtroom using his/her own technical means or in the courtroom of a particular court and cannot change the method determined by the party to the case, since the above may lead to a violation of the functional

[69] Judgement of the Civil Cassation Court in structure of the Supreme Court of 14 April 2021, case № 343/1397/19 (proceeding № 61-13703св20), Judgement of the Civil Cassation Court in structure of the Supreme Court of 09 October 2020, case № 320/463/17 (proceeding № 61-41837св18).

[70] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 16 November 2021, case № 910/8690/20, Judgement of the Commercial Cassation Court in structure of the Supreme Court of 18 May 2021, case № 923/378/17.

[71] Judgement of the Civil Cassation Court in structure of the Supreme Court of 28 March 2023, case № 711/7486/19 (proceeding № 61-10183св21).

[72] Judgement of the Criminal Cassation Court in structure of the Supreme Court of 13 June 2023, case № 225/127/17 (proceeding № 51–3295 км 22).

principles of civil proceedings[73]. If a participant's motion to take part via the conference in the courtroom of another court is granted, the obligation to ensure the possibility of actual participation of the litigant in the hearing shall be imposed on the court entrusted with conducting the videoconference[74].

While positively assessing the introduction of videoconferencing as one of the modes by which a court hearing can be held, since in some cases it is the only possible means of personal participation in the proceedings, i.e. ensuring the right to a fair trial, we would like to point out some of the drawbacks that it has, in our opinion. Firstly, participation in a court hearing via videoconference using one's own technical means is possible provided that the person has an electronic digital signature that allows for identification and connection to the relevant services. At the same time, obtaining an electronic digital signature has certain limitations, for example, for foreign citizens who are outside Ukraine. Secondly, the quality of communication, which, of course, is a technical problem, does not always allow the court to respond in a timely manner to motions filed by the parties to the case and to fully perceive the information provided. Thirdly, modern technologies do not allow to examine the evidence submitted by the parties to the case in court, as the above results in a violation of the principle of immediacy[75].

Summarizing the abovementioned, it should be noted that the current procedural legislation and case law are gradually increasingly using information technology in civil proceedings. Despite the existing problems, national courts are trying to take into account the ECHR case law on the right to a fair trial as much as possible.

[73] Judgement of the Civil Cassation Court in structure of the Supreme Court of 10 May 2023, case № 208/6136/15 (proceeding № 61-1861св23).

[74] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 26 January 2022, case № 537/5256/19 (proceeding № 61-634св21).

[75] Judgement of the Commercial Cassation Court in structure of the Supreme Court of 30 March 2023, case № 905/2307/21 (905/496/22*)*.

ChatGPT as a Tool for Litigants and their Lawyers: Quo Vadis?

Tetiana Tsuvina*

Abstract: The article examines the potential applications of ChatGPT in legal proceedings, with a particular focus on its use by litigants and their attorneys in the preparation of procedural documents. The article is structured in three parts: the first part provides a general overview of the use of artificial intelligence, in particular ChatGPT, in court proceedings with focus to recent cases of such use in the practice of foreign countries; the second part analyses the first Ukrainian case in which the Supreme Court qualified the use of ChatGPT by a party of the case during the preparation of procedural documents as an abuse of procedural rights and disrespect of court; in the third part of the text, the author attempts to analyze the use of ChatGPT in drafting procedural documents and presents arguments in favor of the erroneous position of the Supreme Court. The author posits that to qualify the use of ChatGPT in the creation of procedural documents as an abuse of procedural rights, it is necessary to demonstrate that the relevant criteria have been met, for example providing false information to the court, and the mere use of modern technologies cannot be qualified as a procedural abuse. The article calls for a broader discussion on the development of uniform standards for the responsible use of AI by legal professionals.

Keywords: Artificial Intelligence; ChatGPT; abuse of procedural rights; civil procedure

1. Introduction

The use of Artificial Intelligence (AI) is steadily expanding into various areas of our daily lives, and justice is no exception. This can

* *Doctor of Science (Law), Head of the Department of Civil Procedure, Arbitration and International Private Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. E-mail: t.a.tsuvina@nlu.edu.ua*

be seen in the increasing efforts of the international community to adopt instruments on this issue, the most prominent of which are the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment (CEPEJ, 2018)[1], Resolution 2341 of the Parliamentary Assembly of the Council of Europe "Need for democratic governance of artificial intelligence" (2020)[2]; Report of the Committee on Legal Affairs and Human Rights "Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems" (2020)[3]; Recommendation of the Council on Artificial Intelligence (Organisation for Economic Co-operation and Development, OECD/LEGAL/0449, 2019)[4]; The Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technology in the judiciary" (2023)[5] etc.

These documents deal with many important aspects of the use of information technologies (IT) and AI in the administration of justice and during trials, the advantages and disadvantages of such use, the types of IT used in this area, the principles for their dissemination, etc. Recently, the analysis of these issues has also been presented in various publications[6], which have focused

[1] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment (CEPEJ, 2018). https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

[2] Resolution 2341 of the Parliamentary Assembly of Council of Europe "Need for democratic governance of artificial intelligence" (2020). http://www.europeanrights.eu/public/atti/Resolution_2341_(2020)_ENG.pdf

[3] Report on Committee on Legal Affairs and Human Rights "Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems" (2020). https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-22-EN.pdf

[4] Recommendation of the Council on Artificial Intelligence (Organisation for Economic Co-operation and Development, OECD/LEGAL/0449 (2019). https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

[5] The Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technology in the judiciary" (2023). https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7

[6] Szekely J. Present and future in the digit(al)ization of judicial procedures in romania in european context. *Acta Universitatis Sapientiae: Legal Studies*, 2021. Vol. 10(2). P. 253–269; Zsolt Z. Big-data-based legal analytics programs. what will data-driven law

mainly on the assistive technologies and the perspectives for the use of AI by judges. Thus, the use of AI to assist parties and their lawyers, as well as the judicial qualification of such actions during trials, remained outside the attention of scholars. However, recent developments in legal practice encourage us to study this issue in the broader context of the impact of IT and AI on the administration of justice and its transformation in terms of international standards of due process and fair trial.

This article is an attempt to explore the potential use of AI, in particular Chat GPT, by parties and their lawyers in drafting court documents and the peculiarities of qualification of such actions by courts. The article consists of three parts: the first part analyses cases of AI, in particular ChatGPT, use by parties of proceedings in different jurisdictions and its qualification by judges; the second part provides an analysis of the first Ukrainian judgment issued by the Supreme Court, which assessed the use of ChatGPT by litigants and qualification of such activity as disrespect of court and abuse of procedural rights; the third part attempts to analyse the use of ChatGPT in terms of procedural rules to prevent improper use of ChatGPT by the parties and their lawyers.

2. ChatGPT and legal practice

In March 2023, the world's tabloids were stirred by the news that an American lawyer, Steven A. Schwartz, had utilised the AI tool ChatGPT to draft various court pleadings. Consequently, the ChatGPT-generated statements included references to court

look like?. *Acta Universitatis Sapientiae: Legal Studies*. 2021. Vol. 10(2). P. 287–302; Dymitruk M. The Right to a Fair Trial in Automated Civil Proceedings. *Masaryk University Journal of Law and Technology*, 2019. Vol. 13 (1). P. 27–44; Veress E. Can justice be anything other than human? *Acta Universitatis Sapientiae: Legal Studies*. 2021. Vol. 10(2). P. 161–168; Razmetaeva Yu., Razmetaev S. Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities. *Access to Justice in Eastern Europe*. 2021. Vol. 2(10) 104–117; Razmetaeva Yu. Algorithms in The Courts: Is There any Room for a Rule of Law. *Access to Justice in Eastern Europe.* 2022. Vol. 4 (16). P. 87–100, etc.

precedents that did not exist, indicating that AI had invented legal positions and incorporated them into the lawyer's statements. The court's response was prompt, with Judge P. Kevin Castel questioning the lawyer about the use of non-existent court positions in his statements. He then imposed appropriate sanctions on the lawyer[7].

Recently more and more legal professionals – both judges and parties' representatives – try to explore the capabilities of AI in the legal field to facilitate and optimize their work. Lawyers and judges alike have sought to understand the capabilities of ChatGPT. For instance, in January 2023, two judges in Colombia opted to present their interactions with ChatGPT as evidence to bolster their judgments. In the first case, the judges used it as part of their argumentation on the merits of the case, which dealt with the fundamental right to health of a child[8]. In the second case, the judge used it to motivate the conducting of the trial via the metaverse and to explain how it would take place[9]. In March 2023, the Punjab and Haryana High Court in India employed the use of ChatGPT to determine a bail plea[10].

[7] *Mata v. Avianca*, Inc. (1:22-cv-01461), District Court, S. D. New York. https://www.courtlistener.com/docket/63107798/mata-v-avianca-inc/; Weiser B. Here's What Happens When Your Lawyer Uses ChatGPT. *The New York Times*. 27 May 2023. https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html; Nowak M. Lawyer Uses ChatGPT in Federal Court and It Goes Horribly Wrong. *Forbs.* 27 May 2023. https://www.forbes.com/sites/mattnovak/2023/05/27/lawyer-uses-chatgpt-in-federal-court-and-it-goes-horribly-wrong/?sh=72a780d63494

[8] Judgement of the 1st Circuit Labor Court of Cartagena. 30 January 2023. https://forogpp.com/wp-content/uploads/2023/01/sentencia-tutela-segunda-instancia-rad.–13001410500420220045901.pdf

[9] Gutierrez J. D. ChatGPT in Colombian Courts. Why we need to have a conversation about the digital literacy of the judiciary. *Verfassungsblog*. 23 February 2023. https://verfassungsblog.de/colombian-chatgpt/

[10] In a first, Punjab and Haryana high court uses Chat GPT to decide the bail plea. *The Times of India.* 28 March 2023. https://timesofindia. indiatimes. com/india/in-a-first-punjab-and-haryana-high-court-uses-chat-gpt-for-deciding-upon-bail-plea/articleshow/99070238.cms

These have raised numerous questions: whether AI can or cannot be used by parties and their lawyers in drafting procedural documents; whether any usage of ChatGPT constitutes an abuse of procedural rights and an act of disrespect of court; whether ChatGPT can be perceived as a reliable source of knowledge; whether can fragments of text created by ChatGPT be inserted into procedural documents; who is responsible for the text created by ChatGPT and inserted into the text of procedural documents – both created by the court or procedural documents of the litigants?

Courts have frequently highlighted the rationale behind the optimisation of the administration of justice as a justification for the use of AI in general and ChatGPR. In one of such cases the judge emphasised that: "The Office will resolve to add the grounds for the resolution of the case based on the construction of texts made in the IA application https://chat.openai.com/chat as an initiative to speed up the resolution of tutela cases. The purpose of including these IA texts is not in any way to replace the Judge's decision. We are really looking for is to optimize the time spent in the drafting of judgments, after corroboration of the information provided by IA"[11].

We should emphasize that while the use of assistive technologies is strongly supported in both the academic literature, by international institutions and among the judicial community, the use of substitute technologies has been treated with caution and the possibility of their use has been questioned. In Opinion No. 26 (2023) of the CCJE, it is observed that the countries surveyed emphasized the importance of maintaining the human element in the decision-making process. This implies that AI should be utilized

[11] Rojas M. L. F., A judge in Cartagena (Colombia) claims to have use ChatGPT as support tool to resolve a guardianship for health care neglect. Foro Administración, Gestión y Política Pública. 03 February 2023. https://forogpp. com/2023/02/03/a-judge-in-cartagena-colombia-claims-to-have-use-chatgpt-as-support-tool-to-resolve-a-guardianship-for-health-care-neglect/

to provide support, rather than to assume the role of judges. In particular, IT and AI can assist judges in making merits assessments and/or predicting the outcomes of proceedings. They can also assist judges in evaluating their conclusions, identifying relevant case law, and assessing it. Additionally, they can provide access to novel or previously unidentified lines of argument, promote consistency in decision-making, and more. At the same time, the principles of judicial independence and impartiality, as well as judicial autonomy, must be respected. Technology should not be used to predict an individual judge's decision-making. Furthermore, decision-making must be carried out explicitly and implicitly only by judges, and not by the AI. To respect judicial autonomy, technology must be used in accordance with the aforementioned principles. The utilisation of data tools as a substitute for judicial legal research and of supportive AI to assist judges in reaching decisions may impede an individual judge's capacity to conduct research and make decisions. The deployment of predictive coding, for instance, may compromise a judge's ability to discern what constitutes relevant evidence and may negatively impact their capacity to assess the strength of evidence. While such tools are designed to facilitate judicial decision-making, they may, over time, diminish judicial expertise and experience[12].

The CCJE supports the use of technology to assist judges within the following principles: 1) the rule of law; 2) judicial independence and impartiality; 3) judicial autonomy; 4) judicial oversight; 5) accessibility and quality; 6) Interoperability and continuous improvement; 7) piloting; 8) non-discriminatory design and operation; 9) transparency and intelligibility; 10) accountability; 11) integrity, security and data protection; 12) openness and

[12] The Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technology in the judiciary" (2023). https://rm. coe. int/ccje-opinion-no-26-2023-final/1680adade7

privacy; 13) funding; 14) training and operability[13]. The European Ethical Charter on the use of AI in justice systems and their environment sets out five key principles for the implementation of AI in justice, which are: 1) respect for fundamental rights; 2) non-discrimination; 3) quality and security; 4) transparency, impartiality and fairness; 5) "under user control"[14].

The idea of the optimisation of judges work due to the usage of IT and AI is popular among policy makers and judges all over the world. But, in our view, the issue of time is open to question. While the profit of such technologies is usually connected with the efficiency purpose, there is also the question of how much time should be spent by a judge or court clerk on text checking and dialog with AI. In principle, now the same information is provided by a clerk, but in case of AI usage all documents should be rechecked by such clerks. In above mentioned cases of creation of the case law it can take even more time for rechecking that the write a text by your own. Correlated concern relates to the reliability of the data. Chat GPT is not designed to provide accurate responses to questions, and, of course, it is not the proper source for legal advises. J. D. Gutiérrez highlighted in this regard that "current LLMs [Large Language Models] are not trustworthy sources of information and should only be used – with the utmost care – when other more effective and safe options are not available. […] the judiciary should promote digital literacy and an informed, transparent, ethical, and responsible use of AI tools, in order to reap its potential benefits and prevent risks"[15]. Last but

[13] The Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technology in the judiciary" (2023). https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7

[14] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment (CEPEJ, 2018). https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

[15] Gutierrez J. D. ChatGPT in Colombian Courts. Why we need to have a conversation about the digital literacy of the judiciary. *Verfassungsblog*. 23 February 2023. https://verfassungsblog.de/colombian-chatgpt/

not the least is the personal data protection concern, because the persons, who put the private information to the ChatGPT should be aware of this issue, which can be of particular importance in criminal or sensitive matters[16]. All in all, the idea to force IT and AI to work for the optimization of administration of justice is good, but in order to do it in an appropriate way we need to develop clear guidelines and rules of the game to minimize negative effects of such innovations.

3. The Ukrainian case

The Ukrainian legal community has recently been rocked by the revelation of the initial judgement concerning the utilization of ChatGPT in the applications of litigants to the court. The judgment has been met with considerable controversy, with legal professionals divided into two opposing camps. One group supports the position of the Supreme Court, which considers the use of ChatGPT for drafting procedural documents to be unacceptable. The other group sees nothing wrong with such use.

From the circumstances of the case, it can be seen that the claimant's lawyer applied to the Supreme Court for a clarification of its previous judgment, in accordance with Art. 245 of the Commercial Procedural Code of Ukraine. In this application, he also referred to the so-called "position" generated by the AI system ChatGPT, which concerned the answer to the questions raised by the court. It can be inferred from the circumstances of the case that the "position" formulated by ChatGPT referred to the concept of "voluntary obligation". This concept was applied in qualifying the defendant's obligation arising from the decision of the general meeting of shareholders. The claimant's representative posited

[16] Hatton M. Hopes ChatGPT will help those representing themselves in court. Newsroom. 06 January 2024. https://newsroom.co.nz/2024/01/06/hopes-chatgpt-will-help-those-representing-themselves-in-court/

that such a term requires clarification, as it contravenes the theoretical concept enshrined in the substantive law, as stated by the AI system ChatGPT. Upon consideration of the application, the Supreme Court determined that the actions of the party's lawyer exhibited a lack of respect for the Supreme Court judges and the judicial system as a whole, and qualified such actions as an abuse of procedural rights[17].

To provide a legal assessment of this situation, it is necessary to consider two key points. Firstly, it is important to examine the procedure for clarifying the court judgment itself. Secondly, it is essential to analyse the way ChatGPT was utilised in this case.

Firstly, the procedure for the clarification of a court judgement, as set out in Article 245 of the Commercial Procedural Code of Ukraine, is designed to ensure the enforcement of binding court judgements. In accordance with Part 1 of Article 245 of the Commercial Procedural Code of Ukraine, upon the request of the parties to the case, a public or private enforcement officer, the court is obliged to clarify the court judgment that has entered into force without changing the content of the court judgment. Such an application may be filed if the court judgment has not yet been enforced or if the period within which the judgment may be enforced has not expired. The essence and significance of this procedure is that those directly involved in the enforcement of a court judgment should be able to apply to the court for an interpretation of its judgment if there are difficulties in the enforcement of such a judgment and it is necessary to have the court explain the issues related to the enforcement of such a judgment, in particular, the methods of its enforcement. In contrast, the claimant's legal representative did not request clarification of the court decision with the intention of ensuring its enforcement. Instead, they

[17] Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22. https://reyestr.court.gov.ua/Review/116984639.

requested an interpretation of the text of the court judgment and, in fact, presented new arguments for the court judgment with *res judicata* effect. It does not correspond to the very essence of the procedure for clarification of a court judgment.

Secondly, it is necessary to analyse the methods and purposes of ChatGPT usage in this case. In this context, the Supreme Court has stated: "The issues to which the applicant seeks clarification under Article 245 of the Commercial Procedural Code of Ukraine relate to the reasons for the judgment and are raised in such a way that they require the court to further justify the judgment already made regarding the legal relationship of the parties that were not the subject of consideration (regarding the procedure for bringing the charter into compliance, the procedure for counting votes at the next general meeting). The applicant actually requested that the Supreme Court either deny or confirm that the AI system "ChatGPT", which is not recognised as a reliable source of scientifically proven information, generated the information in question. This was contrary to the conclusions made by the court in the court judgment. In this manner, the applicant questioned the judge's discretion and judicial interpretation of this issue in a judgment that had become final, thus disregarding the authority of the judiciary"[18].

In addition, the Supreme Court offers general observations on the attitude towards the use of AI in court proceedings and the judiciary. First, the Supreme Court emphasized that "AI can be a useful and assistive tool in the field of justice, but it cannot replace the role of judges. Technology should only be used to support and strengthen the rule of law"[19]. Analysing

[18] Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22 – https://reyestr.court.gov.ua/Review/116984639.

[19] Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22. https://reyestr.court.gov.ua/Review/116984639.

the party's procedural actions in this case, the Supreme Court pointed out that the party had used AI inappropriately – not to facilitate the administration of justice, but rather to undermine the court's conclusions and judgment. It further emphasised: "[…] The fact that a party to the proceedings, in a procedural statement, opposes the conclusions of the Chamber of Judges of the Supreme Court on a legal issue and the AI system, which has no regulatory framework and no scientifically proven basis for use, as a basis for explaining a court judgment, inevitably raises problems in terms of the impact on the authority of the Supreme Court, its case law and confidence in the judiciary in general. It is the fundamental duty of judges and lawyers to observe the rules of procedure and the principles of fair trial. Lawyers, aware of the role of the Supreme Court in a democratic society, are expected to exercise a high degree of professional diligence and to cooperate constructively with the Court in order to prevent the filing of deliberately unfounded complaints (applications). The deliberate or negligent misuse of court resources, including the use of AI without a proper understanding of its capabilities as a basis for opposing its conclusions to those of the court, may undermine public confidence in the judicial system. Such conduct is contrary to the purpose of the right to apply to the court"[20]. The Supreme Court considered that the applicant's actions, taken as a whole, showed a lack of respect for the judges. As a result, the judges found the application to be manifestly groundless and manifestly unfounded. In fact, it is reduced to disagreeing with the Court's judgment, re-examining the Court's conclusions with a different legal interpretation and answering questions that were not the subject of the dispute. Such actions were also found to be inconsistent with the task of commercial litigation

[20] Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22. https://reyestr.court.gov.ua/Review/116984639.

and were qualified as an abuse of the right to file an application under Article 43 of the Commercial Procedural Code of Ukraine[21].

This judgment of the Supreme Court is quite controversial, as the Supreme Court actually qualified the use of the ChatGPT in the trial as an abuse of procedural right and disrespect for the court, which has the implication that it is inadmissible to oppose the position of the Supreme Court and the ChatGPT. It should be noted that in the above-mentioned American case, the ChatGPT essentially included non-existent and invented precedents in the text of procedural documents, thereby actually misleading the court and the other party. Instead, in the Ukrainian case, the party was blamed for inserting AI-generated text fragments into procedural documents? How does the latter case differ from the situation in which a person who is not a legal expert presents his or her arguments in an opinion, having previously used information from the internet, or even presenting his or her own understanding of the text of the law, perhaps having previously researched the issue in certain academic sources or case law reviews, which are in public access? In this case, should we apply different standards to ordinary citizens who are parties to a case and to legal professionals involved in the case (lawyers, prosecutors, etc.) and, finally, should we apply the same standard of impossibility of using ChatGPT to all legal professionals – both judges and lawyers?

In our view, the situation is not quite so clear-cut, and not all attempts by the parties and their representatives to use AI in general and ChatGPT in particular should be considered the disrespect of court and the abuse of procedural rights. Notably, in this case there was a dissenting opinion by Supreme Court Judge Hanna Vronska, who stated in part: "[…] The current legislation on commercial proceedings does not prohibit the use of AI technologies

[21] Ухвала Касаційного господарського суду у складі Верховного Суду від 8 лютого 2024 року у справі № 925/200/22. https://reyestr.court.gov.ua/Review/116984639.

in commercial proceedings. In addition, court practice lacks an established approach and clear criteria by which the use of AI by litigants can be recognised as an abuse of procedural rights. […] I consider that by referring to the responses generated by ChatGPT in order to substantiate its position, taking into account the content of the application, the arguments and the reasoning contained therein, the applicant has not shown disrespect to the Court and has not questioned its conclusions, on the contrary, it has sought to establish and clarify certain conclusions on the issues on which the Supreme Court has expressed its opinion. The statement does not contain any humiliating, insulting or other negative statements, open demonstration of disrespect for the Court, etc. The mere reference to the information generated by AI technologies, in the absence of other reasonable circumstances indicating unfair procedural actions of a person, cannot be recognised as an abuse of procedural rights. Considering the above, in my opinion, the Supreme Court has prematurely recognised the filing of an application for clarification of the court's decision as an abuse of procedural rights by giving an excessively harsh assessment of the applicant's actions"[22]. This case demonstrates that the judicial system's stance on the use of AI in procedural documents is yet to be fully defined.

4. Does any use of ChatGPT constitute a disrespect to the court and abuse of procedural rights?

In our view the principle of "under user control" should be extended to encompass the use of ChatGPT by parties and lawyers.

[22] Окрема думка судді Верховного Суду Вронської Г. О. у справі № 925/200/22. 08 лютого 2024 року. https://reyestr.court.gov.ua/Review/117074064?fbclid=IwAR1Qlz-_LguEXYcD-EJbVb-5-hNO9jlVCw3Ucm4FcuP4P9Te1D2rWgVci9M_aem_ATD8yNfuIhUMsr1cS9Mj3Km4NWFET0CzJM2SVWm5pdP_BOskeMlS-SoMtqlZTovpG8t2J1oKWjkjRVMR7VengUtQ

This implies that the litigants are accountable for their applications and actions.

In the case of the use of chat GPT by the parties of the trial to draft procedural document it is necessary to distinguish between the ways in which the relevant technologies can be used. Firstly, it is possible to utilise ChatGPT to paraphrase and reformulate text. Secondly, it is possible to instruct ChatGPT to perform more complex tasks, such as asking legal questions and providing legal advice, drafting procedural documents with relevant answers and references to relevant case law, and so on. In the first case, ChatGPT is essentially used as a text editorial assistant, and in the second case, as a text author. In our opinion, the question of the admissibility of using ChatGPT in the texts of procedural documents should not be raised in general, but taking into account the specific circumstances of the case. If a person uses ChatGPT for the purpose of editing the text, reformulating, paraphrasing, composing, etc., and the use of technology is subject to further control and verification of the person, then it is unlikely that the use of ChatGPT and, more generally, AI is contempt of court, abuse of procedural rights, etc. Such behavior, in our opinion, is permissible. If ChatGPT or AI is used to generate text, its fragments, and is used to build the framework of legal argumentation, especially with reference to certain precedents, then the assessment of the actions of the parties to the case should be more thorough. In the cases cited above, when, for example, lawyers used ChatGPT to create legal texts, which resulted in submitting applications to the court with reference to non-existent precedents, we are undoubtedly talking about negligence committed by a lawyer. In view of the above, in our opinion, the principle of "under user control" should be applied, and there should undoubtedly be a person who is responsible for such actions.

In this context, the principle "under user control" should be interpreted as the obligation of a party to the case or a lawyer to be responsible for their actions in utilising the GPT chat, to verify

the information generated by the latter. Does a person have to inform the court about the use of the source of information in this case? It is unlikely that the individuals have any such procedural obligation, because even the absence of a reference to the law is not a ground for denial of justice according to Ukrainian law. Consequently, a person cannot be denied consideration of a claim on this basis since the task of the court is to properly assess and qualify the relevant legal relations.

It is also of great importance to determine what should be considered an abuse of procedural rights and contempt of court. In academia literature, the abuse of procedural rights is often defined as the conduct of the parties or their representatives within the civil procedure, which has the purpose of achieving an outcome that is contrary to the aim of civil procedure. While not all countries have enshrined the notion of procedural rights abuses in their procedural legislation, such actions can be sanctioned by the court in many national orders. To illustrate, in 2017 Ukrainian procedural legislation identified the inadmissibility of abuse of procedural rights as one of the principles of civil and commercial proceedings (subpara 11 para 3 art 2 of Commercial Procedural Code of Ukraine, subpara 11 para 3 art 2 of Civil Procedural Code of Ukraine). This principle is set forth in a provision that litigants and their representatives shall utilize procedural rights in good faith; abuse of procedural rights is not permitted.

In accordance with the specific circumstances of the case, the court may recognise the following actions as an abuse of procedural rights: 1) filing an appeal against a court decision that cannot be appealed, is not in force and has expired, filing a motion (application) to resolve an issue that has already been resolved by the court, in the absence of other grounds or new circumstances, filing a groundless recusal or committing other similar actions aimed at unreasonably delaying or impeding the trial or enforcement

of a court decision; 2) filing several lawsuits against the same defendant(s) with the same subject matter and on the same grounds, or filing several lawsuits with the same subject matter and on the same grounds, or committing other actions aimed at manipulating the automated assignment of cases to judges; 3) filing a manifestly unfounded claim, a claim in the absence of a subject matter of dispute or in a dispute that is obviously arbitrary; 4) unreasonable or arbitrary joinder of claims for the purpose of changing the jurisdiction of the case, or deliberately unreasonable involvement of a person as a defendant (co-defendant) for the same purpose; 5) the conclusion of a settlement agreement aimed at harming the rights of third parties, intentional failure to notify the persons to be involved in the case. If the filing of a motion, complaint, or application is found to be an abuse of procedural rights, the court has the right to leave such motion, complaint, or application without consideration or return it, taking into account the circumstances of the case (art 43 of the Commercial procedural Code of Ukraine, art 44 of the Civil Procedural Code of Ukraine).

Despite this actions, in case law of Supreme Court different procedural actions were qualified as an abuse of procedural rights, for example, the use of foul language, offensive and abusive words or symbols by litigants in documents submitted to the court and in communication with the court (judges) and other litigants[23]; submission to the court of receipts confirming payment of court fees that have already been used in other cases, knowing in advance that they will not be credited to the State Budget[24]; the withdrawal of a claim after the execution of a settlement agreement or the repeated submission of an application for the

[23] Постанова ВП ВС від 07 листопада 2019 року у справі № 9901/324/19. https://reyestr.court.gov.ua/Review/85775709

[24] Постанова ВС від 03 листопада 2020 року у справі № 530/1630/18. https://ips.ligazakon.net/document/C015740

approval of a settlement agreement at the stage of reviewing a decision to deny such an application[25], etc.

It is not difficult to see that all the above actions are committed contrary to the aim of civil or commercial proceedings, in order to mislead the court or to delay the process, etc. At the same time, in our opinion, the actions of a litigant to apply to the ChatGPT to clarify disputed points of law may be considered careless, reckless, but not as an act of disrespect towards the court or an abuse of procedural rights. An alternative approach could result in the conclusion that any arguments presented in appeals and cassation appeals by self-represented parties lacking the requisite legal expertise could be regarded as a "*court v. unreliable source*" opposition and constituting an abuse of procedural rights.

At the same time, when discussing legal professionals, it is imperative that the standard of conduct be more rigorous, given that they are bound by the requirements of legal professional ethics. It is evident that these individuals should be held to a higher standard of accountability for the content of the procedural documents submitted to the court. Therefore, in the event of the thoughtless utilization of case law created by a ChatGPT, the lawyer in question should be subject to disciplinary action.

Another general concern regarding the utilisation of AI by lawyers is the confidentiality and protection of personal data. In Opinion No. 26 (2023) of the CCJE, it is emphasised that the utilisation of AI may be opaque with regard to the nature and manner of the utilisation of information by such technology[26]. To generate texts, participants in the trial should provide the system

[25] Постанова ВС від 04 березня 2020 року у справі № 712/13890/15-ц (провадження № 61-15953св19 https://protocol.ua/ua/postanova_ktss_vp_vid_04_03_2020_roku_u_spravi_712_13890_15_ts/

[26] The Opinion No. 26 (2023) of the Consultative Council of European Judges (CCJE) "Moving forward: the use of assistive technology in the judiciary" (2023). https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7

with the specific information pertaining to the merits of the case, including sensitive information. In the future, such information may be used by AI, and in fact, it is out of the lawyer's control and the lawyer cannot ensure its safety or attorney-client privilege. It is of paramount importance that lawyers are aware of this potential issue and take the necessary steps to prevent the leakage of information when utilising AI. Taking this into account, we can agree with the J. D. Gutierrez, who calls for the development of certain standards for the use of AI by legal professionals. Among such standards the author identifies the following: "(i) the user must understand how the technology works, acknowledges its limitations and risks, and makes sure that the tool is adequate for the required task (informed use); (ii) the user is transparent about the use of the technology in proceedings (transparent use); (iii) the user distinguishes clearly which sections of the judicial decision or legal document are AI-generated text (ethical use); and, (iv) the user rigorously checks information retrieved from the AI system against reliable sources and explicitly informs about such examination (responsible use)"[27].

5. Conclusion: Quo vadis?

Today, we can already see the first reactions of the courts to the use of ChatGPT within applications filed to the court. Thus, the Ukrainian Supreme Court considers such actions as an abuse of procedural rights and disrespect for the court. American courts also consider it to be disrespectful to the court with corresponding sanctions. At the same time, sometimes courts also try to take some preventive measures. For example, after the cited case in the United States became known, a judge of the Fifth Circuit

[27] Gutierrez J. D. ChatGPT in Colombian Courts. Why we need to have a conversation about the digital literacy of the judiciary. *Verfassungsblog*. 23 February 2023. https://verfassungsblog.de/colombian-chatgpt/

Court of Appeals proposed to enshrine in the Rules of Court the rule that persons applying to the court must make a reservation in their statements that they did not use AI when writing statements to the court[28]. Notably, in Ukrainian legislation we can also find some preventive measures for particular procedural abuses. For example, Civil Procedural Code of Ukraine enshrined the measure used to prevent the manipulation of jurisdiction and automated case distribution. Thus, in accordance with subpara 10 para 3 art 175 of the Civil Procedural Code a claimant should confirm in his claim that he/she has not filed other claim(s) against the same defendant(s) with the same subject matter and on the same grounds.

However, the positions of the Ukrainian Supreme Court and American Fifth Circuit Court of Appeals seems to presume that any use of AI in legal proceedings is automatically unappropriated behaviour. However, it is hardly reasonable to agree on this, given the different ways in which AI is used by litigants and their lawyers. In our view, the accent should be not on the usage of the ChatGPT or AI in the trial (as a tool for generation text or paraphrasing it), but rather on that fact that even if there were such usage whether it was under humans' control and whether the legal professionals check the text. Thus, in our opinion, the use of GPT chat in court proceedings by the parties to the case and their representatives should be qualified as abuse of procedural rights and contempt of court not only because of the conditional opposition "court authority vs. ChatGPT", but if there are features of abuse of procedural rights.

[28] Ambrogi B. In First for A U. S. Appeals Court, 5th U. S. Circuit Court Considers Rule Requiring Lawyers to Certify they Did Not Rely on AI to Create Filings. *LawSites.* 29 November 2023. https://www.lawnext.com/2023/11/in-first-for-a-u-s-appeals-court-5th-u-s-circuit-court-considers-rule-requiring-lawyers-to-certify-they-did-not-rely-on-ai-to-create-filings.html

Digital Transformation of Criminal Proceedings: Key Vectors and Problems of Realization

Oksana Kaplina*, Iryna Krytska**

Abstract: In summary, the article identifies the main vectors of digital transformation of criminal procedure and analyses them with due regard to the possible benefits of digital technologies in criminal proceedings and the potential risks which they may pose. In particular, among the areas of optimization of the criminal procedural form from the standpoint of the use of digital technologies during pre-trial investigation or trial of criminal proceedings, the authors reveal the aspects related to the use of video conferencing technologies during procedural actions and in court; the authors also clarify the peculiarities of implementation of a possible model of electronic criminal proceedings; analyze the current state of national legislation on the functioning of the Unified Judicial Information and Telecommunications System. In addition, the authors focused on the problems of digitalisation of evidential means and their legislative "formalisation", including an attempt to determine the place of digital media among other types of evidential information, highlighted the controversial aspects of procedural actions aimed at obtaining digital information, and provided proposals for a conceptual change in approaches to the assessment and use of digital sources of evidential information in criminal proceedings. Finally, the article reveals the theoretical and empirical aspects of ensuring the observance of human rights in criminal proceedings in the context of their digital transformation, with a particular focus on ensuring the right to digital privacy and the right to property in the context of seizure of digital media in criminal proceedings. Within the framework of the latter issue, the author reviews the relevant case law of the ECHR, key scientific achievements on this issue, and identifies and critically analyses legislative trends in this area.

* *Doctor of Science (Law), Professor, Criminal Procedure Department, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. E-mail: o.v.kaplina@nlu.edu.ua*

** *PhD (Law), Lecturer, Criminal Procedure Department, Yaroslav Mudryi National Law University, Kharkiv, Ukraine. E-mail: i.o.krytska@nlu.edu.ua*

Keywords: electronic criminal proceedings; videoconference; digitalisation; digital evidence; assessment of digital evidence; right to privacy

1. Introduction

Actualisation of scientific interest in the issues related to the use of digital technologies in criminal proceedings is determined by several factors. First, along with the rapid growth of the number of so-called "cybercrime" ("cybergrooming", "carding", "card trapping", "cash trapping", "software skimming", etc.), which may be caused by the fact that ordinary Internet users leave a significant amount of digital information online, including their personal data, telephone numbers, bank payment cards, bank accounts even when solving crimes that are "traditional" for the criminal justice system, the pre-trial investigation of such crimes faces a gap in the regulation of the peculiarities of collecting and verifying "digital evidence" and its evaluation in court proceedings. Secondly, the level of legislative support aimed at regulating aspects related to the collection of digital evidence, its research, evaluation and use in criminal proceedings clearly keeps pace with the rapid development of digital technologies, and most importantly, the protection of human rights in the new digital reality. Thirdly, despite the significant attention of criminal procedure law scholars to the problems of legalisation of digital reality[1], it must be noted that domestic scholars mainly focus

[1] O. Kaplina, S. Sharenko, *Access to Justice in Ukrainian Criminal Proceedings during COVID-19 Outbreak*, In *Access to Justice in Eastern Europe*, 2/3 (7), 2020, 115–133; S. Kovalchuk, *Vchennia pro rechovi dokazy u kryminalnomu protsesi: teoretyko-pravovi ta praktychni osnovy: monohrafiia*, Suprun V. P., Ivano-Frankivsk, 2017, 618; I. Krytska, *Rechovi dokazy u kryminalnomu provadzhenni : monohrafiia*, Edit A. Tumaniants, Pravo, Kharkiv, 2018, 280; D. Litkevych, *Teoretyko-pravovi osnovy vykorystannia dosiahnen naukovo- tekhnichnoho prohresu u kryminalnii protsesualnii formi : dys. PhD*, Yaroslav Mudryi National Law University, Kharkiv, 2020, 280; O. Metelev, *Hnoseolohichna i pravova*

their intellectual efforts on certain segments of the use of digital progress in a particular area of law or a particular legal institution (material evidence; documents; committing crimes with the help of digital technologies, electronic currencies, malicious software, etc.) The above indicates that criminal procedure law lacks a comprehensive scientific study that would systematically address the "digital problems" of modern criminal procedure relevant to the increasing digitalisation of society and a fundamental change in approaches to national digital security, cybersecurity and the transformation of criminal procedure with due regard for them.

It is reasonable to point out separately the key areas of digital transformation, the scale of which should be equal to the scale of transformations in criminal procedural legislation, otherwise the problems will remain without their legislative solution, and law enforcement practice without proper legal instruments. In particular, the following vectors may be considered: (1) optimisation of the criminal procedural form, use of digital technologies during pre-trial investigation or trial of criminal proceedings; (2) resolution of issues related to digitalisation of evidential means and their legislative "formalisation", since investigation of criminal offences committed with the use of technical means requires the use of unorthodox, innovative methods; (3) ensuring respect for human rights during criminal procedure in the context of its digitalisation.

pryroda tsyfrovykh dokaziv u kryminalnomu protsesi, in *Pravova pozytsiia*, 1 (20), 2018, 75–86; O. Metelev, *Zbyrannia tsyfrovoi informatsii yak okremyi sposib otrymannia dokaziv pid chas kryminalnoho provadzhennia*, in *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia parvo*, 20, 2020, 177–180; V. Myltseva, *Elektronne pravosuddia: vynyknennia ta perspektyvy rozvytku: dys. PhD*, Kyiv, 2020, 202; A. Skrypnyk, *Vykorystannia informatsii z elektronnykh nosiiv u kryminalnomu protsesualnomu dokazuvanni : dys. PhD*, Yaroslav Mudryi National Law University, Kharkiv, 2021, 379; A. Stolitnii, *Elektronne kryminalne provadzhennia: peredumovy vynyknennia, suchasnyi stan ta perspektyvy rozvytku : monohrafiia*, ArtEk, Kyiv, 2016, 724.

2. The use of digital technologies during pre-trial investigation or trial of criminal proceedings to optimise the criminal procedural form

Moving on to the analysis of the first aspect, we should note that the development of digital technologies has contributed to the optimisation of the criminal procedure form. The Criminal Procedure Code of Ukraine has introduced new modern technologies that simplify criminal proceedings. Namely, firstly, the current CPC enshrines the rules governing the possibility of conducting procedural actions in criminal proceedings remotely. Thus, it provides for the possibility of conducting interrogation and identification by video conference during the pre-trial investigation (Article 232), regulates the procedure for conducting remote court proceedings (Articles 336, 354), and regulates the procedure for interrogation at the request of a competent authority of a foreign state by video or telephone conference (Article 567). However, given that the CPC requires the use of technical means and technologies to ensure proper image and sound quality, as well as information security (i.e. security of information and supporting infrastructure), a person participating in the proceedings must be either in the office of the pre-trial investigation body or court, or in a pre-trial detention facility or penitentiary.

In the light of the mentioned above, attention should be paid to the guarantees that must be ensured when conducting procedural actions in the mode of videoconference. They can be conditionally divided into guarantees aimed at ensuring the constitutional rights of a person and guarantees related to the effective pre-trial investigation. Specifically, the first group may include: (1) establishing a list of grounds for interrogation and identification using video communication (including the right to protection of life and health); (2) ensuring the right to professional legal aid; (3) protection of information transmitted via communication

channels during a videoconference and the inadmissibility of unlawful interference with it. The second group includes guarantees that ensure: (1) the use of appropriate software and hardware; (2) the engagement of a specialist in remote procedural actions; (3) regulation of the possibility of interrogating a person not only in specially appointed places and using stationary equipment, but also from any place where the person is located and using his or her own technical means (which is currently already regulated for other types of proceedings).

Secondly, the Verkhovna Rada of Ukraine finally approved the draft Law on Amendments to the Criminal Procedure Code of Ukraine to ensure the gradual implementation of the Unified Judicial Information and Telecommunication System (reg. No. 8219 of 23 November 2022), No. 3604-IX of 23 February 2024)[2], functioning of which is intended to ensure electronic document flow in addition to the existing advantages in the form of automated distribution of criminal proceedings and jury selection; provision of information to legal entities and individuals on the status of consideration of materials in criminal proceedings; issuing documents; transferring materials to an electronic archive; preparation of statistical data; registration of correspondence; centralised storage of texts of procedural documents.

Thirdly, Decree of the Ministry of Internal Affairs of Ukraine No. 257 of 16 March 2020 established the "SLID" ("TRACE") information and telecommunication subsystem, which aims to record information on objects seized during investigative (detective) actions in a single information space using modern information technologies, computer and telecommunication equipment; provide information and analytical support to the activities of

[2] Draft Law (UA) No. 3604-IX of 23 February 2024.on Amendments to the Criminal Procedure Code of Ukraine to Ensure the Phased Implementation of the Unified Judicial Information and Telecommunication System.

police bodies (units) aimed at preventing and investigating criminal offences; establishing links between data relevant to criminal proceedings; ensuring information processing on objects seized during investigative (detective) actions, filling and maintaining up-to-date information resources of databases (databanks) included in the information subsystem of the National Police[3].

Regarding the optimisation of the criminal procedural form, it can be stated that criminal proceedings are somewhat conservative in terms of creating digital infrastructure, unlike other types of procedural branches. This is due to the specifics of criminal proceedings, the need to respect the rights and legitimate interests of persons involved in criminal proceedings, and strict adherence to the criminal procedural form under the risk of having the obtained evidence declared inadmissible. However, the digital world is testing the strength of the classical requirements of the criminal procedural form and is gradually winning, proving the superiority of digital technologies that provide speed, convenience, and cheapness, and interest in the use of digital technologies is growing as paperwork that can be replaced by digital documents increases, and as models for simplifying the recording of procedural actions can be introduced, etc.

An attempt to introduce criminal proceedings in electronic form seems to be obviously prospective. In this context, it should be added that on 30 April 2020, the pilot eCase system of electronic criminal proceedings was launched as part of a pilot project in the anti-corruption bodies – the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's Office and the High Anti-Corruption Court of Ukraine. This system integrates

[3] Order of the Ministry of Internal Affairs of Ukraine (UA) No257 of 16 March 2020 on Instruction on the formation and maintenance of the information subsystem "SLID" of the information and telecommunication system "Information Portal of the National Police of Ukraine".

with existing automated systems and document flows in Ukraine that are required in criminal proceedings. The system will allow judges and investigating judges to access the system, including in court, for additional research of evidence and key positions in the proceedings, access to materials in electronic form and upload them to their own court information systems. The prosecutor's office will be able to provide procedural guidance online; investigative units will receive full automation of "paper, manual" investigation processes, will be able to promptly analyse all the necessary information; other participants in criminal proceedings will receive the necessary documents in electronic format[4]. Thus, a full-fledged electronic criminal proceedings system has been introduced in a test mode. After a certain period of its operation, it is preferable to obtain a detailed analysis of the eCase system, its advantages and risks. Such an analysis is necessary to decide whether it is reasonable to introduce a digital format of document flow in criminal proceedings by any pre-trial investigation body.

The advantages of possible electronic criminal proceedings may include: 1) increased accessibility of procedural information for the majority of participants in criminal proceedings while creating additional opportunities for their interaction. In particular, this includes the possibility of filing, approving and resolving motions electronically, as well as filing challenges, etc. It should be emphasized that an additional guarantee of the right of participants in criminal proceedings to access procedural information ultimately affects the degree of real security of the rights and freedoms of each participant in the criminal proceedings; 2) the previous advantage leads to the following – reduction of the criminal proceedings by decreasing the time for sending procedural documents (motions, complaints, rulings,

[4] *Systemu elektronnoho kryminalnoho provadzhennia eCase zapustiat vzhe 30 kvitnia*, on *LegalHub.online,* 8 April 2020.

resolutions, etc.), transferring criminal proceedings to the court for application of measures to ensure criminal proceedings. It also cuts down the time for the parties to the proceedings to get acquainted with the criminal proceedings, as it becomes possible to do so at any time (not just during working hours), anywhere and simultaneously by all parties to the proceedings; 3) e-proceedings will have an indirect positive impact on the procedural capabilities of defence counsels in criminal proceedings, since, for example, defence counsels can remotely send procedural documents to the prosecution, investigating judge, court to be admitted as evidence, review the criminal proceedings, file complaints electronically, etc. Obviously, this will help to reduce the time spent by defence counsel and their expenses, and thus may have a positive impact on the availability of qualified legal aid for suspects and accused persons. This also applies to representatives of the victim, civil plaintiff, civil defendant, third party, etc.; 4) optimisation of material costs during the proceedings (postage, costs of making copies of the proceedings, legal aid costs, some procedural costs, etc.). This may apply to both the transfer of materials from the prosecution to the court and between courts of different levels; 5) significant reduction of the risk of falsifications and corrections in criminal proceedings, especially when it comes to procedural documents already posted on the electronic portal, and thus indirectly increase the transparency of justice in criminal cases.

Concluding the analysis of the issue of the prospects for the introduction of electronic criminal proceedings, we would like to emphasise a possible model that would take into consideration foreign experience in this regard. Therefore, based on the analysis of the experience of functioning of electronic systems of criminal justice authorities in the USA (“Oasis”, “Magic Lanter”, “Fluent”), England (“Transforming Through Technology”), Germany (“INPOL-neu”, “rsCASE”), Belgium (“e- Justice”, “Tax-on-

Web"), as well as generalisation of foreign scholars' approaches, A. V. Stolitnyi proposed to create a Corporate Information and Analytical Automated (Electronic) Criminal Justice System (CIAS CrimJust), which should cover all stages of criminal proceedings and all subjects of criminal proceedings and integrate electronic information resources of the state to the maximum extent possible[5].

3. Resolving issues related to the digitalisation of evidence and its legislative formalisation

Moving on to the second aspect highlighted above, in particular, related to the issues of digitalisation of means of evidence and their legislative "formalisation", we will identify possible areas of adaptation of criminal procedural evidence law to the digital realities of today and the challenges of the near future, given that the formation of evidence is inseparable from the potential restriction of a person's rights, and therefore, it is important to properly regulate it. In addition, the relevant provisions of the CPC are characterised by a certain outdatedness compared not only to similar regulations in the legislation of other states, but even to other procedural branches of law (administrative, commercial, civil). Therefore, we will outline the prospective directions of development:

(1) *Determining the place of digital information and its media in the system of procedural sources of evidence.* In light of this, it is worth pointing out that there is a significant plurality of approaches to this issue in the theory of criminal procedure: from the attempt to attribute this category of objects to traditional procedural sources of evidence (only documents, or only material evidence, or both, depending on what kind of information is of

[5] A. Stolitnii, *Vdoskonalennia elektronnoho sehmenta kryminalnoho provadzhennia*, in *Kryminalno-protsesualne pravo ta kryminalistyka, 2 (2),* 2017, 187–191.

evidentiary value in criminal proceedings) to the recognition of the urgent objective need to distinguish digital sources of evidentiary information as an independent procedural source.

In line with the foregoing discussion, it should be noted that due to the absence of a constant connection between digital information and its material storage medium, it is difficult to deny the existence of such specific features as translatability (the ability to be transferred from one medium to another), multiplicity (possibility of existence of the same information simultaneously on different, unrelated and unconnected media), as well as variability (possibility of being deleted, fully or partially changed, etc. in the absence of direct "physical" access or without human intervention at all using appropriate software). Therefore, in our opinion, it is more appropriate not to try to "fit" digital information and its media into the system of evidence and its procedural sources that has been unchanged for several decades, but rather to recognise its specificity, to acknowledge these objects as having independent evidentiary value and, accordingly, to expand the range of procedural sources of evidence.

This issue becomes particularly relevant given the appearance of completely new, entirely non-objective, intangible manifestations of evidentiary information, for example, the so-called "digital trail", which can be viewed as a certain chain of traces in the information and telecommunications network consisting of several chronologically arranged and logically connected records of digital information through the switching equipment of the telecommunications operator(s) from a digital medium, for example, of the offender to the digital medium of another person, for example, the victim. Furthermore, we would like to draw attention to the rules that must be observed when collecting and examining such digital evidence as a digital trace: (1) engagement of a specialist in the course of procedural actions during which

relevant information may be detected (search, inspection, removal of information from electronic information systems, temporary access to things and documents); (2) consideration of restrictions regulated by subpara. 2 para. 1 Art. 159, para. 2–4 of Part 2 of Article 168 of the CPC of Ukraine regarding the ways of access to digital media and the exclusive grounds for their seizure; (3) given that the digital trail itself is not available for direct presentation and examination during the trial, it is necessary to engage an expert and conduct an examination (including to identify destroyed information, establish the facts of unauthorised access to it, its alteration, distortion, etc.).

(2) *Expansion of legally regulated methods of forming evidence in criminal proceedings.* We are referring to a significant update of the system of methods of collecting and examining evidence enshrined in the criminal procedure law. In our opinion, the introduction of single-point changes, such as the rules on mandatory participation of a specialist in the course of investigative (detective) actions, during which the issue of obtaining digital information and seizure of its material carriers may arise, is not able to fully respond to the current information technology reality.

In light of this, the issue of ensuring the prompt receipt and use of this type of information and its media as evidence in criminal proceedings remains relevant, and on the other hand, preventing unlawful and unjustified violations or restrictions of the rights and legitimate interests of individuals and legal entities. In this regard, it should be added that, despite the fact that Ukraine ratified the Convention on Cybercrime on 07 September 2005[6], certain provisions of this international treaty have not yet been implemented in national legislation. In view of this, it is particularly relevant to analyse some of the proposals formulated in draft law

[6] Convention on Cybercrime ETS No. 185 of 23 November 2001.

No. 4003 of 01.09.2020[7], which were directly aimed at resolving this issue.

Thus, the aforementioned draft law proposed to introduce a new measure to ensure criminal proceedings in the national CPC, namely, "urgent preservation of information". A systematic analysis of these proposals requires attention to certain aspects, including:

(1) the use of the term "information" in the title of the measure. Indeed, it seems more appropriate to use the term "data", since, firstly, it is used to refer to this measure in Article 16 of the Convention on Cybercrime. And, secondly, such a designation would be more appropriate, since data can be transformed into information by analysing, identifying connections, highlighting the most important facts, and synthesising them; that is, information is data transformed into a meaningful form for appropriate use. Meanwhile, at the moment of application of such a security measure, analysis and selection are not yet taking place, and therefore it is more correct to speak of the concept of "data";

(2) inappropriateness of limiting the list of *corpus delicti* in criminal proceedings in respect of which this measure of restraint may be applied. Comparing this list with Articles 2–10 of the Budapest Convention shows that the drafters of the law have intended to cover only those crimes that are expressly mentioned in these provisions. However, it should be noted that according to Article 14(2) of this international treaty, such measures are appropriate not only for criminal offences established in accordance with Articles 2–11 of the Convention (paragraph a), but also for other criminal offences committed with the help of computer systems (paragraph c). In this context, it is possible to mention the possibility of committing even certain crimes against human life

[7] Draft Law (UA) 4003 of 1 September 2020.on Amendments to the Criminal Procedure Code of Ukraine and the Code of Ukraine on Administrative Offences to Improve the Effectiveness of Countering Cyber Attacks

and health with the use of computer systems and networks (for example, incitement to suicide through correspondence on social networks). In view of this, we propose to consider expanding the list of criminal offences in criminal proceedings in respect of which urgent preservation of information is allowed.

It also seems relevant to analyse the proposals to establish a procedure for temporary access to urgently stored information. A study of the content of the proposed wording of part 3 of Article 159 of the CPC, which provides an opportunity for the investigator, prosecutor to obtain temporary access to certain types of urgently stored information on the basis of their decision without the decision of the investigating judge, indicates that the definition of the list of such information is quite abstract, leaving considerable discretion for law enforcement. Instead, Articles 17 and 18 of the Convention on Cybercrime clearly define the scope of such information, while distinguishing that disclosure of data on the movement of information is an integral part and a logical continuation of the procedure for urgent data preservation, and therefore does not require a separate decision, which ensures maximum efficiency in obtaining such data by the investigator or prosecutor.

However, the submission procedure (Article 18 of the Convention on Cybercrime), which is similar in its legal content and purpose to such a measure to ensure criminal proceedings enshrined in the national criminal procedure legislation as temporary access, regulates the procedure for providing data on the type of communication service used, its technical provisions and the period of service usage; the identity of the service user, postal or geographical address, telephone and other access number, information on bills and payments, which can be obtained through the service agreement or arrangement; any other information on the location of the communication equipment, which can be obtained through the service agreement or arrangement.

In this regard, in our opinion, this may be a more appropriate way to resolve this issue. However, in this case, it should be borne in mind that temporary access should be granted under such conditions only on the basis of a decision of the investigating judge. In our opinion, such a more precise implementation of Articles 17 and 18 of the Budapest Convention (according to which the essence of such a conventional measure as urgent preservation and partial disclosure of traffic data is that the telecommunications service provider that has received an urgent preservation order promptly discloses such amount of traffic data as will be sufficient to enable identification of other providers and establish the "route" of communication) will increase the effectiveness of the application of the relevant measures.

The issue of relevant means of collecting evidence should also be discussed in detail. Particularly, it is worth highlighting that over the past few years, cases of the so-called "'inspection of a digital device" (smartphone, tablet, computer, etc.) in criminal proceedings have become widespread in order to identify and copy digital information stored on these media for its research and use in criminal proceedings. Having seized a certain digital device (phone, computer, tablet) and inspecting this object, the investigator usually does not limit himself to visual observation of its external features (which is an inspection of the object in its traditional sense), but tries to obtain information of a different nature – about SMS messages, messages in Viber, WhatsApp, Telegram, listen to recorded telephone conversations (as some smartphones provide such a function).

The nature of such actions essentially means interference with a person's private communication, which requires mandatory judicial control. In addition, it is obvious that the inspection of an object in its classical sense as a visual observation of the features of a certain material object does not correspond to the nature of the

actions that are conducted in order to investigate the information that may be stored in the relevant device.

We would also like to emphasise that in 2022, the criminal procedural legislation was amended to specifically regulate the issue of detection, seizure and recording of digital information as evidence in criminal proceedings – namely, a number of changes were introduced to part 6 of Art. 236 of the CPC of Ukraine, which regulates the procedure for obtaining access to the contents of computer systems or their parts, mobile terminals of communication systems, including the possibility of overcoming logical protection systems, during a search, as well as to part 2 of Article 237 of the CPC of Ukraine, which sets out the basic requirements for the inspection of computer data. At the same time, as noted above, in the aforementioned circumstances, it may be not only an inspection, but also other ways of getting acquainted with digital information. Besides, the name of the relevant investigative (detective) action – "inspection of computer data" – may significantly narrow the range of potential objects of inspection, since it would be more appropriate to use the word construction "inspection of digital data" or "inspection of digital information" in this context.

In connection with this, it should be noted that currently Article 19 of the Convention on Cybercrime provides for such a measure as a search of a digital device, which is obviously more in line with the nature of the procedural action to be conducted in this case. Discussing this perspective, A. V. Shylo emphasises that since the information contained on electronic devices seized during the procedural actions cannot be identified with the electronic device itself as its physical storage medium, it is a separate object of property rights and the object of the right to privacy, and therefore its seizure and/or copying requires a separate court decision – a decision of the investigating judge to engage an expert to conduct

an examination[8]. Without denying the rationality and validity of the aforementioned suggestions, in our opinion, it is still more appropriate to apply in this case the procedure for temporary access to digital information by means of reviewing and copying it. Moreover, if such access requires overcoming logical protection (i.e., a digital device is password protected), then it is necessary to involve a specialist.

In the context of this suggestion, we also support A. Skrypnyk's conclusions about the need to adapt the experience of certain countries to the national criminal procedure legislation regarding the adoption of the closed container rule, which would provide for two-stage judicial control over the restriction of a person's right to secrecy of communication[9].

(3) *Modification of conceptual approaches to verification and evaluation of evidence in criminal proceedings.*

The current level of technological development of society shows that many of us have a significant amount of personal information stored in smartphones, tablets and laptops, and almost everyone always has some kind of "gadget" equipped with high-quality sound, photo and video recording. Moreover, the vast majority of streets and buildings are equipped with CCTV, and cars are equipped with devices that can record changes in speed, time and location in space, as well as video recorders. Thus, almost anyone can situationally become a "collector" of evidentiary information that will potentially be relevant for establishing the circumstances of a criminal offence.

[8] A. Shylo, *Vykorystannia v kryminalnomu provadzhenni vidomostei, otrymanykh u rezultati provedennia nehlasnykh slidchykh (rozshukovykh) dii: avtoref. dys. PhD*, Yaroslav Mudryi National Law University, Kharkiv, 2019, 14.

[9] A. Skrypnyk, *Pravylo "zakrytoho konteineru" v ukrainskykh pravovykh realiiakh. Kryminalnyi protses: suchasnyi vymir ta prospektyvni tendentsii,* in *II Khark. kryminal. protsesual. poliloh : prysviach. aktual. pytanniam zastosuvannia zakhodiv zabezpechennia kryminal. Provadzhennia*, Pravo, Kharkiv, 2020, 179–181.

In our opinion, this gives rise to an urgent need to change the conceptual views on the regulation of the procedure for verification and evaluation of digital evidence. Indeed, it is obviously necessary to give preference to technical guarantees of verification of the authenticity of information provided to the court as evidence over compliance with the purely formal requirements of admissibility of evidence. The point is that, provided that technical capabilities allow to confirm the authenticity of digital information, it may have evidentiary value.

Instead, sometimes the preference for the unconditional necessity to comply with the formal requirements of the procedural registration of evidentiary information over its significance, strength, value for proving the circumstances relevant to criminal proceedings still occurs in law enforcement practice. However, it seems that, especially in relation to digital evidence, this view should be shifted towards the ability to verify the authenticity of electronic information rather than formalised requirements for its recording. In this context, it is also worth paying attention to the main arguments against this kind of reasoning. They are usually of a technical nature and are limited to the fact that such information is unreliable because it is multiplicative and broadcast, and therefore easily changed, and in certain cases it is difficult to establish its authenticity, as well as to identify the facts of falsification and fabrication of evidence, the content of which is such information.

However, the above arguments can be countered by the fact that verifiability is the main feature of digital sources of evidence, since when they are used, there are sufficiently significant opportunities to verify their identification and authentication using technical means, and verification of the integrity and immutability of information on a digital medium is of a technical nature, which significantly reduces the role of the subjective factor. In fact, while digital information can sometimes be altered

with the help of application software, such interference can just as easily be established by conducting an appropriate expert examination.

To continue our study, it seems appropriate to analyse the meaning of the concepts that we have already used but have not found their disclosure – "authentication" and "verification". A systematic analysis of national legislation gives grounds to state that laws and regulations in various fields contain more than ten definitions of each of these concepts. It would seem that for criminal procedural purposes, authentication of digital evidence should be understood as the process of establishing the identity, similarity of the information contained therein, its origin, integrity and immutability, and verification of digital evidence should be considered as its examination, research aimed at establishing the reliability of the information contained therein and confirming the absence of facts of its unlawful change (modification).

It seems that it is essential to determine the necessary ways and means of authentication and verification of digital evidence. In light of this, first of all, it should be noted that the International Organisation on Computer Evidence has developed some principles in this direction, namely: (1) when working with digital evidence, all general forensic procedural principles must be observed; (2) actions to examine seized digital evidence must not alter it; (3) if it is necessary to provide someone with access to the original digital evidence, such a person must be properly trained and instructed; (4) all activities related to the confiscation (seizure), access, storage and transfer of digital evidence must be fully documented and available for review; (5) the person in possession of the digital evidence is fully responsible for all actions taken with respect to this evidence[10].

[10] Digital Forensics: Guidelines, on the website https://gjerrud.com/digital_forensics/guidelines.html

Obviously, for the verification of digital evidence, it will be important to record in detail the characteristics of the software (e.g., type of operating system and its registration number), as well as the digital information itself (e.g., file type, size, time of creation, time of editing, time of opening, user information, etc.) The protocol should also contain the software used to ensure the integrity (immutability) of the data. This includes, among other things, the principle of hashing (hash function). An important element of the toolkit for verifying the reliability of digital evidence is computer forensics. By the way, the use of the hash function is currently considered to be one of the main conditions that makes it possible to use a copy of digital information in proving. Particularly, I. G. Kalancha and A. M. Harkusha emphasise the ability to verify (check) a copy of information by hashing the primary information, a copy of information and comparing the obtained hash values. It is stated that this provides an opportunity to mathematically verify and confirm the integrity and authenticity of a copy of information recorded on the target electronic storage medium. Along with compliance with the requirement that the primary information being copied may not be amended before, during and after copying by connecting the electronic storage medium to a specialist's or investigator's computer, which is done "in read-only mode", for example, with the use of a record locking device, the abovementioned provides unique conditions for guaranteeing the integrity and authenticity of the copy data, and, accordingly, collecting admissible evidence. It is also emphasised that hashing – the calculation of checksums to verify data integrity – should be recorded directly in the protocol of the procedural action (i.e. the values obtained during hashing)[11].

[11] I. Kalancha, A. Harkusha, *Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty*, in *Yurydychnyi naukovyi elektronnyi zhurnal, 8,* 2021, 338.

The issue of examining copies of digital information in court and using them as proper and admissible evidence in proceedings has recently become a subject of analysis for the Supreme Court (hereinafter – the SC). Particularly, the Joint Chamber of the Supreme Court expressed its opinion on this issue in its decision of 29 March 2021 (case No. 554/5090/16-к). The judges pointed out the groundlessness of identifying electronic evidence as a means of proof and the material carrier of such a document, referring to the characteristic feature of an electronic document – the lack of a strict link to a specific material medium[12].

Referring to the provisions of the Law of Ukraine "On Electronic Documents and Electronic Document Management", the Joint Chamber noted that each of the electronic copies is considered an original electronic document if it is stored on several electronic media; however, the same electronic document may exist on different media. Therefore, all copies of an electronic document identical in content may be considered as originals and differ from each other only in time and date of creation. Interestingly, the judges also emphasised the ability of the authorised person who created the electronic document to identify it as an original by using special software by calculating the checksum of the file or directory with files (CRC-sum, hash-sum). In addition, for this purpose, special research may be provided[13].

In another case, the Criminal Court of Cassation of the Supreme Court (Ruling of 26 January 2021, court case No. 236/4268/18) also stressed that a material storage medium is only a way to store information, which is relevant only when an electronic document is material evidence. They also pointed to the main feature of

[12] Judgment of the Joint Chamber of the Supreme Court of Ukraine of 29 March 2021, case No. 554/5090/16-к.

[13] Judgment of the Criminal Court of Cassation of the Supreme Court of 26 January 2021, case No. 236/4268/18

an electronic document, which is the absence of a strict link to a specific material medium. The judges noted that the DVD-R discs attached to the case file were produced in connection with the need to provide information that is relevant in criminal proceedings and is an independent source of evidence derived from information stored on a computer in electronic form in the form of files. Thus, an electronic file in the form of a video file recorded on an optical disc is an original (representation) of an electronic document[14].

Consequently, there is a clear trend towards the formation of new, modern views on the use of digital information as evidence in criminal proceedings in court practice. Moreover, the SC judges themselves draw attention to the shortcomings of the domestic criminal procedure legislation in this regard, pointing to the need to update it as soon as possible, since it is the court practice that should now bridge the existing gaps, including on the conditions and procedure for using not only copies of digital media in evidence, but also other types of digital evidence, such as screenshots, information from open sources, etc.[15].

In view of the aforesaid, we would like to stress the urgent importance of amending the criminal procedure legislation, which would not only define a special new procedure for collecting and recording digital information, but also introduce new approaches to the study of this type of evidence, shifting the focus from formal rules to the possibility of verifying digital information for its authenticity and immutability using hashing technology. Furthermore, it is advisable to point out the potential use of such a method of authentication and verification of digital information as the "chain of custody". The essence of this technology is the

[14] Judgement of the Criminal Court of Cassation of the Supreme Court of 26 January 2021, case No. 236/4268/18.

[15] *Suddi KKS VS obhovoryly problemni pytannia dopustymosti elektronnykh dokaziv pid chas sudovoho rozghliadu,* on the official website of the Supreme Court, *Judiciary.*

step-by-step registration of all information about the identification properties, production, storage and movement of a file from user to user, up to the examination in court – and, if necessary, demonstration of this to the participants in the process. Thus, it is a step-by-step documentation of the file's identification properties from the moment of its registration, broadcast, storage and transfer from one medium to another.

Quite interesting in the light of our work are the recommendations formulated in Module 4 "Introduction to Digital Forensics" (developed within the framework of the Education for Justice (E4J) initiative, which is a component of the Global Programme for the Implementation of the Doha Declaration, United Nations Office on Drugs and Crime (UNODC), Vienna, 2019). More specifically, it is proposed to divide all digital evidence into 3 groups and provide appropriate advice for each of these categories: 1) content generated by one or more persons (e.g., text of an email, word processing documents) – may be considered admissible evidence if it is reliable and credible (i.e., it can be attributed to any person); 2) content generated by a computer or digital device without the user's participation (e.g., data logs) – may be considered admissible if it can be shown that the device was functioning properly at the time of data generation and if it can be shown that security mechanisms were operating at the time of data generation to prevent data alteration; 3) content generated simultaneously by the user and the device (e.g., dynamic spreadsheets in programs such as Microsoft Excel) – both of the previous rules must be applied[16].

Therefore, taking into account the aforementioned tools and recommendations when using digital evidence in criminal

[16] *Module 4 "Introduction to Digital Forensics"* (developed by the Education for Justice (E4J) initiative, a component of the Global Programme for the Implementation of the Doha Declaration, United Nations Office on Drugs and Crime (UNODC), Vienna, 2019.

proceedings will facilitate the algorithmisation of the procedure for its verification, and thus will further shift the focus in terms of verification and assessment of evidence regarding its admissibility from compliance with purely formal requirements during collection to establishing an opportunity for its identity and authenticity.

4. Ensuring respect for human rights in criminal justice in the context of its digital transformation

With regard to the last third focus area of our work, which is devoted to the issues of ensuring the observance of human rights during criminal proceedings in the context of its digital transformation, we believe it is appropriate to draw attention to the following.

For example, when considering the issue of holding a court hearing via videoconference, we should also address the problem arising in law enforcement practice, such as ensuring the rights of the accused and witnesses who are remotely present during the court hearing.

Particular attention should be paid to the realisation of the accused's right to defence during interrogation via videoconference, as well as the right of a witness to use the legal assistance of a lawyer during testimony (Article 42(2)(3) of the CPC of Ukraine; Article 66(1)(2) of the CPC of Ukraine). Restrictions in this regard, introduced primarily in connection with the pandemic, may affect the ability to exercise this right, as the CPC of Ukraine still does not specify where the defence counsel of the accused and the witness's lawyer should be located: next to the person to whom he or she provides legal assistance, in the courtroom, or can also join a video conference call, fulfilling the distance requirements and being in the office or at home. By the way, the realisation of the right to a confidential meeting between the defence counsel and the client before interrogation

remains problematic. As a prospective direction, given the rapid development of modern communication technologies, as well as the threats faced by society in connection with the emergence of extremely dangerous viral diseases, care can be taken to create or allocate a separate communication channel or create other technical capabilities to ensure communication between the defence counsel or lawyer and the accused or witness in order to fulfil their right to confidential communication.

Challenges may also arise if the suspect, witness, or victim subject to interrogation does not speak the language of the proceedings. The engagement of an interpreter requires that the person being interrogated find out the level of language proficiency and, if necessary, object to the interpreter. It seems that in order to decide on the level of proficiency of the interpreter in the relevant language, it is also necessary to provide time for preliminary communication between the above persons, which is significantly complicated during a "remote" trial.

Among the rights that may be subject to significant interference, which is sometimes disproportionate, in the course of criminal proceedings under the conditions of their digital transformation, the right to respect for private and family life, enshrined in Article 8 of the European Convention on Human Rights, namely its elements such as respect for private life and correspondence, should obviously be mentioned.

In this regard, it is advisable to pay attention to the lack of unity of interpretation of the provisions of Article 31 of the Constitution of Ukraine and Article 14 of the CPC of Ukraine. In particular, Article 14 of the CPC of Ukraine adds "other forms of communication" to the objects of protection specified in Article 31 of the Constitution of Ukraine, i.e. "correspondence, telephone conversations, telegraph and other correspondence". In addition, the Criminal Procedure Law also clarified the purpose of the respective interference by

adding "detection and prevention of serious and especially serious crimes".

Interpretation of the above legislative provisions and their comparison makes it possible to assume that the Constitution of Ukraine, adopted on 28 June 1996, could not have provided for all the specifics of secrecy of communication, while Article 14 of the CPC of Ukraine (which, as we know, was adopted on 13 April 2012) is formulated not only on the basis of the fundamental provisions of the Constitution, but also taking into account the general conceptual approaches to building a new model of criminal procedure, establishing judicial control and the system of general principles of law. This article is taking into account the general conceptual approaches to the construction of a new model of criminal procedure, the enshrining of judicial control, the system of general principles, Chapter 21 "Covert investigative (detective) actions", as well as the provisions of international instruments ratified by Ukraine and the case law of the European Court of Human Rights[17].

From this perspective, we would like to emphasise that the European Convention on Human Rights itself uses the concept of "correspondence", but the functional interpretation of this concept has been given by the ECHR, which has repeatedly expressed an approach to its broad understanding in its judgments. In particular, the ECHR in its judgements states: "The concept of 'correspondence' is broadly defined. It also includes correspondence between the defendant and the lawyer[18]; information contained on a computer's hard drive[19]. The ECtHR

[17] O. Kaplina, A. Tumaniants, *ECTHR decisions that influenced the criminal procedure of Ukraine,* in *Access to Justice in Eastern Europe*, 1, 2021, 102–121.

[18] European Court of Human Rights Judgment. Niemietz v. Germany, App. No. 13710/88 (1992).

[19] European Court of Human Rights Judgment. Roemen and Schmit v. Luxembourg, App. No. 51772/99 (2003).

addressed the concept of "correspondence" in its judgment of 05.09.2017 in the case of Bărbulescu v. Romania (application no. 61496/08). Specifically, the judgment stated that "with regard to the concept of 'correspondence' in the text of Article 8 of the ECHR, this word is not accompanied by any adjective, unlike the word 'life', which is used in the text of Article 8 with the adjectives "private and family life"[20]. Thus, the ECtHR formulates a broad approach to understanding the content of this concept. In the case of Roman Zakharov v. Russia, the ECtHR stated that "telephone conversations are covered by the concepts of 'private life' and 'correspondence' within the meaning of Article 8 of the Convention"[21]. To sum up, the ECtHR broadly interprets the concept under consideration, which, in our opinion, is justified, since forms of instant communication will only increase with the further development of modern technologies, changing the mechanism of communication, technical means of its use, but not the very essence of communications and the right to privacy.

This conclusion is important given that the scientific literature expresses separate opinions on the need to differentiate procedural access to "open" and "unopened" correspondence[22], as well as on the non-inclusion of e-mails, SMS or MMS messages opened and read by the owner, which, according to the ECHR practice, should be considered personal documents, in the correspondence[23].

On the other hand, the point of view of A. V. Skrypnyk, who notes that in the case under consideration, "judicial control should

[20] European Court of Human Rights Judgment. Petri Sallinen and Others v. Finland, App. No. 50882/99 (2005).

[21] European Court of Human Rights Judgment. Bărbulescu v. Romania, App. No. 61496/08 (2017).

[22] European Court of Human Rights Judgment. Roman Zakharov v. russia, App. No. 47143/06 (2015).

[23] D. Serhieieva, O. Starenkyi, *Vykorystannia rezultativ nehlasnykh slidchykh (rozshukovykh) dii dlia provedennia tymchasovoho dostupu do rechei i dokumentiv*, in *Visnyk kryminalnoho sudochynstva*, 4, 2015, 70–80.

concern the legality of access not to the digital data carrier as a whole, but to electronic messages. Such a conclusion is consistent with: a) the object of legal protection of the rights under consideration – electronic messages as files; b) foreign experience. For example, the US courts, based on the doctrine of "plain view" adapted to digital evidence, "compare a computer to a closed container (suitcase, chest, briefcase), the contents of which are not available for inspection until a law enforcement officer takes action, that clearly go beyond the reasonable expectations of the owner of the information" (switch on the phone screen, open files stored on the device, etc.), and therefore "the examination of the information content of electronic media requires a court order to conduct a search". Particularly interesting is the position of some US district courts that equate a digital data carrier as a whole with a separate file contained on it, rather than a "closed container". This approach is: a) due to the fact that "computers contain so much information relating to various areas of a person's life that the possibility of "mixing" documents and consistent intrusion into privacy increases when the police collect evidence on a computer"; b) aimed at preventing unjustified expansion of the scope of search for information on electronic media"[24]. In this context, it should only be added that judicial control must relate to the lawfulness of access to electronic messages received on a communication device from any software products aimed at ensuring communication between persons.

Finally, it should be noted that the seizure of digital media in criminal proceedings may also be considered an interference with property rights. In this regard, it is important that the guarantees of this right are balanced with the achievement of the effectiveness

[24] A. Skrypnyk, *Vykorystannia informatsii z elektronnykh nosiiv u kryminalnomu protsesualnomu dokazuvanni : dys. PhD*, Yaroslav Mudryi National Law University, Kharkiv, 2021, 171–172.

of criminal proceedings – prevention of unlawful and unjustified violations or restrictions of human rights (to privacy, secrecy of correspondence, property, business, etc.) and their legitimate interests in cases where such digital media must be seized to fulfil the tasks of criminal proceedings. Therefore, in this aspect, it will be crucial to build a mechanism for restricting the rights of a person when obtaining digital evidence media that would allow finding the necessary balance between the ability to conduct an effective pre-trial investigation and bring perpetrators to criminal liability, on the one hand, and the interests of persons who may suffer significant damage when applying, in particular, measures to ensure criminal proceedings in respect of their property, on the other hand.

It is worth pointing out that in previous years, several draft laws were developed, none of which was ever adopted, which were aimed at amending the criminal procedure legislation regarding the application of certain measures to ensure criminal proceedings to digital media. This is, for example, the draft law "On Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding improvement of the procedure for applying certain measures to ensure criminal proceedings)" (Reg. No. 9484 of 17 January 2019.)[25] and the draft law "On Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding improvement of the procedure for applying certain measures to ensure criminal proceedings)" (Reg. No. 2740 of 15.02.2020)[26].

However, the aforementioned draft laws, unfortunately, did not demonstrate a balance in the issue we have indicated.

[25] Draft law No. 9484 of 17 January 2019 on Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the procedure for applying certain measures to ensure criminal proceedings).

[26] Draft law No. 2740 of 15 February 2020 on Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the procedure for applying certain measures to ensure criminal proceedings).

Nevertheless, by analysing some of their shortcomings, we can try to illustrate a more balanced model of legal regulation. Thus, the idea of supplementing paragraph 4 of part six of Article 100 of the CPC of Ukraine with new paragraphs four, five and six raises certain reservations. In particular, these provisions provided for the obligation to "return to the holder (legal owner) or transfer to them for safe keeping material evidence that does not contain traces of a criminal offence in the form of devices for processing, transmission and storage of electronic information or their components, if they are used as objects or means of labour and/or the seizure of which may cause significant damage to their holder (legal owner)"[27]. It should be emphasised here that the return of material evidence to the holder (legal owner) results in the restoration of the relevant powers arising from the ownership right, and therefore is one of the ways to decide the status of material evidence. Therefore, the return means that the material object passes into the full use and disposal of the relevant person with the right to alienate or even destroy it. It is clear that such actions cannot be taken in relation to material evidence, as in this case the principle of direct examination of testimony, things and documents during the trial will not be ensured.

The drafters of the bills have also made attempts to limit the ability to seize property if it is digital media, but despite the obvious positive aspects, in our opinion, such proposals also carry potential risks. Thus, as it stands, the current version of subpara. 3, part 2, Article 168 of the CPC of Ukraine prohibits the temporary seizure of electronic information systems or their parts, mobile terminals of communication systems, except when their provision together with the information contained therein

[27] Draft law No. 9484 of 17 January 2019 on Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the procedure for applying certain measures to ensure criminal proceedings).

is a prerequisite for conducting an expert investigation. At the same time, draft Law No. 9484 provides for a significant limitation of this option, which is undoubtedly important for the collection and verification of evidence in criminal proceedings. Particularly, a systematic analysis of the proposed amendments to Article 98(4), Article 167(3), Article 168(2) of the CPC of Ukraine shows that only those devices for processing, transmitting and storing electronic information that were themselves an instrument, means or object of a criminal offence can be seized. If only the electronic information contained in them is of evidentiary value, it should be copied "on the spot", without seizure, even temporarily, of its material carriers. It seems that this approach leaves out situations where it is simply impossible to find and reproduce electronic information that could be relevant to establishing the circumstances of criminal proceedings, which was stored on the devices but was destroyed. Taking appropriate actions requires a computer forensic examination to be carried out on a stationary basis with the use of special forensic research methods and special software.

We would also like to draw attention to the controversial, in our opinion, proposal to expand part 5 of Article 170 of the CPC of Ukraine with a new paragraph two, according to which "seizure of property in the form of devices for processing, transmission and storage of electronic information or their components, if they are used by their holder (or legal owner) as objects or means of labour or if their seizure may cause damage to an individual or legal entity that is not a party to this criminal proceeding"[28] is allowed to be imposed only if one of the following purposes is met: 1) to ensure special confiscation; 2) to ensure confiscation

[28] Draft law No. 9484 of 17 January 2019 on Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the procedure for applying certain measures to ensure criminal proceedings).

of property as a form of punishment or a measure of criminal law against a legal entity.

In practice, a common approach is caused by the misidentification of the seizure of certain material objects and the removal of such objects from the actual possession of a person. However, according to Article 170(1) of the CPC, "seizure of property is a temporary deprivation of the right to alienate, dispose of and/or use property by the decision of an investigating judge or court, until it is cancelled in accordance with the procedure established by this Code", i.e. it does not refer to deprivation of the person of such a right as actual possession. Therefore, the seizure of devices for processing, transmitting and storing electronic information will not mean their seizure and deprivation of the person's ability to use them as objects or means of labour, but will only be aimed at preventing their damage, destruction, alienation to other persons, etc.

Consequently, it seems appropriate to distinguish between the existence of grounds for seizure of property and the ability to transfer such property for safekeeping to the owner. Thus, in these situations, the following algorithm of actions may be proposed: if the grounds provided for in Article 170 of the CPC of Ukraine, the mentioned devices may be seized, but only with restriction of the right to dispose of them; the device or its components shall be transferred to the holder (or legal owner) for safekeeping, and the decision on the transfer shall specify the person's obligations regarding the storage of such material object, namely a) to keep material evidence in proper condition suitable for use in criminal proceedings; b) prohibition to alienate it, transfer it to other persons; c) to provide material evidence to the investigator, prosecutor, court for the necessary procedural actions upon request.

5. Conclusions

The article identifies the main areas of digital transformation, namely: (1) optimisation of the criminal procedural form, use of digital technologies during pre-trial investigation or trial of criminal proceedings; (2) addressing issues related to digitalisation of means of proof and their legislative "registration"; (3) ensuring respect for human rights during criminal proceedings in the context of their digital transformation.

It highlights the guarantees which must be observed when conducting procedural actions via videoconference: in particular, those aimed at ensuring the constitutional rights of an individual and those related to the effective pre-trial investigation. The authors also formulate the rules that must be followed when collecting and examining such digital evidence as a digital trace.

Counterarguments to the proposals set out in the draft laws on the implementation of certain provisions of the Convention on Cybercrime are provided. Specifically, it is substantiated that the approach to limiting the list of *corpus delicti* in criminal proceedings in respect of which a potentially new measure of ensuring criminal proceedings, i.e. "urgent preservation of information", may be applied is questionable. The authors state that there is an urgent necessity to amend the criminal procedure legislation which would determine not only a special new procedure for collecting and recording digital information, but also introduce new approaches to the examination of this type of evidence, shifting the emphasis from formal rules to the ability to verify digital information for its authenticity and immutability using hashing technology. In this regard, for criminal procedural purposes, the authors propose to understand the authentication of digital evidence as the process of establishing the identity, similarity of the information contained therein, its origin, integrity and immutability, and the verification of digital evidence as its verification, research aimed at establishing

the reliability of the information contained therein and confirming the absence of facts of its unlawful change (modification).

Finally, the authors prove the need to maintain a balance between the guarantees of property rights (in particular, with regard to tangible objects which are carriers of digital information) and the achievement of the effectiveness of criminal law. It is determined that in this aspect, the leading role will be played by the construction of such a mechanism for restricting the rights of a person when obtaining digital evidence media which would allow finding the necessary balance between the possibility of conducting an effective pre-trial investigation and bringing perpetrators to criminal liability, on the one hand, and the interests of persons who may suffer significant damage when applying, in particular, measures to ensure criminal proceedings in respect of their property, on the other hand.

Наукове видання

ЄВРОПЕЙСЬКІ ФУНДАМЕНТАЛЬНІ ЦІННОСТІ У ЦИФРОВУ ЕРУ

Монографія

(Англійською та українською мовами)

Редакторки:
Размєтаєва Юлія Сергіївна
Філатова-Білоус Наталія Юліївна

Підписано до друку 19.08.2024. Формат 60×84/16.
Ум. друк. арк. 18,5. Обл.-вид. арк. 13. Тираж 100 пр. Зам. № 158

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20, (063) 254-50-84
Вебсайт: https://pravo-izdat.com.ua
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт»,
вул. Весніна, 12, Харків, 61023, Україна
Тел. (057) 717-25-44
Свідоцтво суб'єкта видавничої справи ДК № 5748 від 06.11.2017