Vol XIV, Issue 1

THE ELSA LAW REVIEW

LEGACY COLLECTION

ELR

VOL XIV, ISSUE 1

THE ELSA LAW REVIEW

LEGACY COLLECTION

ELSA Law Review is published by the European Law Students' Association.

The publication may be cited as [2022] ELSA LR 1. ISSN: 2415-1238 (e-version)

Editor in Chief:	Samira Safarova *Vice President in charge of Academic Activities of the International Board of ELSA 2021/2022*
Deputy Editor in Chief:	Ekaterina Kasyanova-Kühl
Academic Editors:	Roberta Rombolà, Parthabi Kanungo
Linguistic Editor:	Maisie Beavan
Technical Editor:	Velina Stoyanova, Julia Karolak
Director for Publications:	Bernadetta Semczuk
Academic Partner:	Católica Global School of Law
Academic Reviewer:	Gonçalo Saraiva Matias *Dean of Católica Global School of Law* Armando Rocha *Associate Dean of Católica Global School of Law*
Website:	https://lawreview.elsa.org

The European Law Students' Association

CATOLICA FACULDADE DE DIREITO ESCOLA DE LISBOA

CATOLICA Global School of Law

All rights reserved. No part of the material protected by this copyright notice may be reproduced, utilised in any form or by any means electronic or mechanical, including photocopying, recording or storing in a retrieval system or transmitted in any form or by any means without the prior permission of the Vice President in charge of Academic Activities of ELSA International. The views expressed by the authors are their own and do not necessarily reflect those of the publishers.

Copyright © The European Law Students' Association and the authors, 2025

CONTENTS

THE ELSA LAW REVIEW LEGACY COLLECTION

This Issue is part of the Legacy Collection, a special edition of the ELSA Law Review comprising of the following issues:

- Volume XII, Issue 2 - written in 2020
- Volume XIII, Issue 1 - written in 2021
- Volume XIII, Issue 2 - written in 2021
- Volume XIV, Issue 1 - written in 2022
- Volume XV - written in 2023
    - containing Volume XIV, Issue 2 - written in 2022

These issues have been collected from 2020 until 2024, but due to publication and internal difficulties not published on schedule. They have now been reviewed and compiled, and are presented here, as part of the Legacy Collection.

The Legacy Collection offers special recognition to authors of articles comprising these issues. Their works are preserved and displayed in the context of the Legacy Collection, which is also meant to contextualise their work into the legal landscape of the years during which it was written.

This Edition also includes a Foreword From the Future, a special addition to the ELSA Law Review to honour authors of these articles and thank them for their contributions.

Below is the list of contributors for the publication of the Legacy Collection.

Publication Coordination:	Niko Anzulović Mirošević *Vice President in charge of Academic Activities of the International Board of ELSA 2024/2025* Velina Stoyanova *Director of Publications, ELSA International Team 2024/2025*
Academic Editors:	Kamil Yusubov, Amil Yafarguliyev
Linguistic Editors:	Amelia Zochowska, Rsaal Firoz
Technical Editor:	Eleni Belogianni
Proofreader:	Julia Karolak

FOREWORD FROM THE FUTURE

Dear Readers,

As we present this long-awaited issue of the ELSA Law Review, we wish to address and sincerely apologise for the significant delay in its release. We know that many of you have been eagerly anticipating this publication, and it is with genuine regret that we acknowledge the impact of this delay on our contributors, readers, and the broader ELSA Network.

This issue reflects the hard work, dedication, and expertise of each contributor who has shared their research and insights. It is a testament to the importance of our mission to promote legal scholarship and cross-border dialogue on human rights issues. Unfortunately, despite the passion and commitment invested by our team, we encountered challenges that led to unforeseen delays. We take full responsibility for this oversight, and we are grateful for your patience.

In response to these setbacks, we have stepped forward to implement crucial improvements to our publication process. We have worked tirelessly to introduce systems and practices that will make our future publications faster and more sustainable. We are confident that our processes are now more robust and equipped to meet the demands of regular, high-quality publication.

With the Legacy Collection, we renew our commitment to providing a platform for meaningful legal discourse and human rights advocacy. We are determined to uphold the standards of excellence that our readers and contributors expect and deserve, and we promise that we will do all we can to ensure that future issues of the ELSA Law Review are published on schedule.

A special thanks goes to all the legal experts in our newly established Academic Board, visible on the ELR website and from ELR XV onwards, who pledge their time and effort to the ELR. Finally, we thank our predecessors and their Publications Teams for identifying flaws with the publication process and giving us the opportunity to remedy them. Thank you all for your support, patience, and trust. We look forward to sharing this and many future issues with you.

Warm regards,

Niko Anzulović Mirošević
Vice President in charge of Academic Activities, International Board of ELSA 2024/2025

&

Velina Stoyanova
Director for Publications, ELSA International Team 2024/2025

LETTER FROM THE EDITORS

Dear Reader,

We are delighted to present *Volume XIV, Issue 1* of the ELSA Law Review, dedicated to human rights law with a special focus on Privacy in the Digital Age. The *ELSA Law Review* (ELR) is a biannual, peer-reviewed, student-edited journal published by the European Law Students' Association (ELSA), under the patronage of Robert Spano, former President of the European Court of Human Rights, and in cooperation with Católica Global School of Law.

As technology reshapes how we live, communicate, and govern, legal frameworks are being pushed to adapt—raising urgent questions about data protection, freedom of expression, and the rule of law.

This issue explores key aspects of these developments. From the GDPR's role in regulating predictive policing and protecting children's data, to the challenges posed by algorithmic content moderation under the Digital Services Act, our contributors address how legal systems strive to keep pace with rapid technological change. The volume also offers a comparative look at hate speech regulation in Germany and the U.S., an analysis of the Italian Constitutional Court's stance on consensual homicide, a discussion on the legality of targeted killings, and reflections on the rule of law in times of crisis.

We thank our Academic Editors Roberta Rombolà and Parthabi Kanungo, Linguistic Editor Maisie Beavan, and Technical Editors Velina Stoyanova and Julia Karolak for their dedicatedwork. We are especially grateful to Bernadetta Semczuk, Director for Publications of ELSA International, for her support throughout this process.

We hope you enjoy reading this edition and find inspiration in the legal debates it presents.

Warm regards,

Samira Safarova
Editor in Chief

&

Ekaterina Kasyanova-Kühl
Deputy Editor in Chief

Volume XIV 2022 Issue 1

AI, LAW ENFORCEMENT AND PRIVACY: DOES THE GDPR SUFFICIENTLY REGULATE FOR AUTOMATED DECISIONS BASED ON PREDICTIVE POLICING PROFILING?

Laura Higgins Mulcahy[1*]

Abstract

Predictive policing is defined as 'any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention'.[2] These activities incorporated in profiling and automated decision-making technologies allow for policing tactics and orchestrated initiatives to be aided by the precision and efficacy of artificial intelligence in order to organise and execute policing forecasts and procedures. Automated decision making in the area of policing can be further incorporated into strategic planning and prioritising either on a macro-level regarding operational intelligence or on a micro-level to make risk assessments in relation to individuals. Broadly speaking, there are two main avenues which automated predictive policing tools can go down. One direction can be to make systematic decisions relating to geolocations of crimes to draw links between places and events and predict where and when crimes are more likely to happen. The other, more contentious direction is using AI to forecast potential perpetrators of crime and to predict who has a higher chance of being involved in future criminal activity. This type of automated profiling can draw on data such as age, gender, marital status and more, and it is this type of data analysis which understandably holds concern for EU data protection law. It is therefore necessary to dissect the GDPR in order to ensure that technologies such as profiling and automated decision making in the area of predictive policing are inherently protected under its regulatory umbrella.

[1*] Author is a Law and Technology LLM student currently studying at Utrecht University.

[2] Aleš Završnik, 'Criminal Justice, Artificial Intelligence Systems, and Human Rights' (2020) 20 ERA Forum, 567 < https://doi.org/10.1007/s12027-020-00602-0> accessed 11 February 2022.

1. Introduction

As a result of globalised digitalisation and innovative artificial intelligence techniques, automated decision making (ADM) has infiltrated almost every aspect of society, from assessing creditworthiness of borrowers to allocating welfare allocation of citizens. The generalised concept of ADM has exhibited promising attributes such as the ability to make work less time-consuming and cost-effective, and to make judgements which are less prone to human error. Nonetheless, ADM in the arena of law enforcement activities and procedures has been generally welcomed by law enforcement actors in light of slicker internet crime techniques such as hacking and scamming, and terrorist propaganda and child abuse material dissemination. This positive consensus has spurred the application of ADM particularly in the area of predictive policing. Whilst Europe has been slower than other jurisdictions such as the US in the adoption of predictive policing technologies, there has already been backlash regarding a European Member States' usage of such technology. An application of Pol-Intel in Denmark has faced recent scrutiny by yielding 'inaccurate and false results […] on the premise of historical data already skewed towards certain ethnic designations based on pre-existing discriminatory practice'.[3] The ADM predictive policing method used by law enforcement authorities in Denmark controversially 'gave physical expression to what had remained an unspoken Danish reality of institutional racism'.[4] This example exhibits the ability for predictive policing outcomes to demonstrate discrimination. It is these data sets which can emerge as contentious, because the question begs, what is the decision-making process behind this discrimination? When a decision is made by artificial intelligence, it is increasingly harder to pinpoint where the accountability lies. With the interplay between ADM and policing techniques gaining traction in Europe, it is important to ensure that they are regulated, and do not infringe the fundamental rights such as the discrimination and consequently privacy. Acknowledging the European fundamental rights *acquis* including the European Charter for Fundamental Rights[5] and the European Convention on Human Rights[6], it is the General Data Protection Regulation[7] (GDPR) which is the main regulatory armour which ought to be applied to issues concerning such data privacy issues. The GDPR remains generally fit for purpose regarding personal data, but because technological

[3] N.T. 'NoTechFor: Forced Assimilation' (*No Tech For Tyrants,* July 2020) <https://notechfortyrants.org/2020/07/13/notechfor-forced-assimilation/> accessed 11 February 2022.
[4] ibid.
[5] Charter of Fundamental Rights of the European Union (2000).
[6] European Convention on Human Rights Act (1950).
[7] Regulation (EU) 2016/679 of the European Parliament (EP) 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).

development and innovation is happening faster than the creation and passage of European laws, there is ample opportunity for lacunas in its protection. With the increased variety of data sets being analysed and utilised by a multitude of public and private actors, it is becoming increasingly necessary to ensure each type of data set is accounted for and regulated by the GDPR. This article will first outline the GDPR articles governing personal data, profiling and automated decision-making respectively *viv-a-vis* data subjects of predictive policing profiling. It will then conclude whether the GDPR satisfies the objectives of data protection in the arena of predictive policing profiling and give commentary as to its effect and potential regulatory mitigation strategies.

2. Predictive Policing and Personal Data Usage

The GDPR lays down rules for the protection of natural persons concerning the processing of their personal data. Personal Data under Article 4(1) is defined as 'any information relating to an identified or identifiable natural person'.[8] From this reading, the definition of personal data has three constituent elements: (1) any information that (2) relates to (3) an identified or identifiable person. The Article 29 Working Party has advised that each of these three elements should be interpreted expansively.[9] It thus suggests that 'any information' can also include information that would be considered 'private' for the purposes of the right to respect for private life. The CJEU stated in *Nowak* that the expression 'any information' is used to reflect the legislature's aim to 'assign a wide scope to that concept'.[10] Acknowledging this, a data subject can 'be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[11] In the context of predictive policing profiling, personal data such as names, geographical and social data are all data elements which relate to an individual and that renders an individual as identifiable. Therefore, it would seem that any type of personal data used for purposes of predictive policing can be justified under the expansive criteria of Article 4(1). However, in order to process personal data of a data subject, or in this context a suspect, there must be a purpose in the form of a legal basis. Article 6 governs the legal basis for personal data. It is questionable under what

[8] ibid art 4(1).
[9] Article 29 Working Party, 'Guidance from the European Data Protection Board' (*Data Protection Commission)* <https://www.dataprotection.ie/en/dpc-guidance/guidance-from-the-european-data-protection-board> accessed 11 February 2022.
[10] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 34.
[11] GDPR (n 7).

criteria the processing of personal data in the context of predictive policing profiling could establish a legal basis. The GDPR allows Member States to enact limitations to specified provisions in certain contexts, notably where necessary to reconcile data protection rights and restricting the application of data protection principles in order to pursue specific purposes, including national security, defence, public security and law enforcement purposes.[12] This is pertinent to the area of predictive policing and data usage as already it can be identified that the processing of personal data in this context is subject to a flexing of the rules laid out in Article 6 of the GDPR. It is therefore up to Member States to account for the legal basis in this context.

3. Profiling and Predictive Policing

Profiling under the GDPR is defined under Article 4(4) as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.[13] In the instance of predictive policing, the data subjects concerned would be those considered to be suspects to police investigations whose data is used to profile them as criminal offenders, of which such profiling is subjected to ADM in order to decipher their likelihood to reoffend. As can be seen from the definition under Article 4 paragraph 4, profiling is an applicable concept which entails the automated processing of personal data for the purpose of evaluating personal aspects to aid decision making about a data subject.[14] Under the GDPR, the concept of ADM overlaps with profiling as they both act on three types of data; data provided by the individual, data observed about the individual and data inferred from the personal information obtained about the individual. ADM can also be defined as 'the process of making a decision by automated means without any human involvement.'[15] These decisions can be based on 'factual data, as well as on digitally created profiles or inferred data.'[16] There is a clear interplay between automated decision making and profiling, so they can be viewed together when analysing the GDPR.

4. Predictive Policing and Automated Decision Making

[12] ibid. art 23(a)-(d).
[13] ibid. art 4(4).
[14] ibid. art 22(4).
[15] Office of the Data Protection Ombudsman, 'Automated Decision Making and Profiling' <https://tietosuoja.fi/en/automated-decision-making-and-profiling> accessed 11 February 2022.
[16] ibid.

Article 22 of the GDPR states, 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'[17] The guidelines of the Article 29 Data Protection Working Party state that for data processing to significantly affect someone the effects of the processing must be that the decision has 'the potential to significantly affect the circumstances, behaviour or choices of the data subjects; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals.'[18] Without question, automated decisions in the context of predictive policing could affect the lives of data subjects, have a long-term impact on them and in the case of biased data sets, result in discrimination of individuals. That would mean predictive policing under Article 22(1) of the GDPR is prohibited. However, a lacuna appears the more that Article 22 is examined. Article 22(2) states that Article 22(1) shall not apply based on several exceptions.[19] These exceptions include contract necessity, explicit consent of the data subject and special categories of data. Article 22(4) goes on to state that Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

5. Exception under Article 9

Article 9(1) states that the 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. However, this prohibition shall not apply under exceptions listed in Article 9(2). Article 9(2)(a) states one of the exceptions being 'The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject' Article 9(2)(g) states, 'Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific

[17] GDPR (n 7).
[18] ibid.
[19] ibid.

measures to safeguard the fundamental rights and the interests of the data subject'. As data subjects (or victims to police investigation) will most likely not provide their explicit consent to be profiled, Article 9(g) is the most appropriate to use in this case. Applying the criteria under 9(g) is necessary, and a step-by-step approach is helpful. In order to justify the processing of personal data revealing racial or ethnic origin (etc.), the criteria to satisfy are:

1. Whether they are necessary for reasons of substantial public interest?
2. Do they have a legal basis under Member State law?
3. Do they respect the essence of the right to data protection?
4. Are they suitable and specific measures to safeguard the fundamental rights and the interests of the data subject?
5. Does predictive policing safeguard the data subjects rights and freedoms?

If these criteria are fulfilled, then a data subject shall not have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

6. Analysis of the Exception Criteria

In order to fully grasp the propensity and give commentary on the aforementioned criteria, it is relevant to answer these questions in the context of predictive policing:

1. Q: Is the profiling necessary for reasons of substantial public interest?
   A: Perhaps profiling in the context of predictive policing is necessary for crime prevention and for protection of the general public against potential criminals.
7. Q: Does the law enforcement authority have a legal basis under Member State law?
   A: This is determined by the individual Member States.
8. Q: Does this type of profiling respect the essence of the right to data protection?
   A: No, it is arguably quite invasive, especially if there is no legal basis given on behalf of a suspect to use this data under Article 4(1).
9. Q: Are there suitable and specific measures in force to safeguard the fundamental rights and the interests of the data subject?
   A: The answer to this is where the data processing seems contentious, because usage of data to profile in this context can lead to an infringement by placing individuals in a category of criminality which could impinge other elements of their private and family life..
10. Q: Does predictive policing safeguard the data subjects rights and freedoms?

A: Not particularly, as it could result in discriminatory outcomes and alternatively it could be viewed as overly-surveillant, which could in turn lead to chilling effects.

In summary, there seems to be more negative than positive answers to justify any sort of exception under Article 22 for the purposes of predictive policing. The European Digital Rights Group criticises the dilution of the right not to be subjected to automated decisions in Art. 22, stating: 'Through profiling, highly sensitive details can be inferred or predicted from seemingly uninteresting data, leading to detailed and comprehensive profiles that may or may not be accurate or fair.'

This dilution can be exhibited in the following breakdown of the Articles as detailed in the earlier passages:

- Article 22(1) prohibits sole automated decision making.
- Article 22(2) gives exceptions to this prohibition.
- Article 22(4) states that special categories of data cannot be permitted in this exception except in situations which comply with 9(2)(a) or 9(2)(g).
- Article 9(1) prohibits *inter alia* processing of personal data based on racial or ethnic origin.
- Article 9(2) permits exceptions to this prohibition.
- Article 9(2)(a) states one of the exceptions being explicit consent (not applicable to predictive policing).
- Article 9(2)(g) states one of the exceptions could be based on necessity to substantiate public interest under Member State law which could indirectly be applied to predictive policing and the prevention of crime and leaving this exception up to Member States for consideration.

Therefore, a Member State can decide that an automated decision making process is permissible based on racial and ethnic origin and it does not violate the GDPR if it is 'necessary for reasons of substantial public interest, on the basis of Union or Member State law.' The principles of being necessary and for public interest are two nuanced terms which ultimately provides member states substantial power in the realm of predictive police profiling.

7. Criticism

To elucidate this observation, in 2021 members of the European Parliament passed a resolution to endorse the report of the Civil Liberties Committee.[20] The report expresses an

[20] Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the Commission's 2021 Rule of Law Report* (2021/2180(INI) <https://www.europarl.europa.eu/doceo/document/LIBE-PR-704642_EN.pdf> accessed 11 February 2022.

opposition to the use of predictive policing tools which operate on artificial intelligence software in order to make predictions about the behaviour of individuals or groups 'on the basis of historical data and past behaviour, group membership, location, or any other such characteristics'. This opposition is based on the fact that predictive policing tools cannot make reliable predictions about the behaviour of individuals.[21] Additionally, the report notes that AI applications have a potential for reinforcing bias and discrimination.[22] Although this resolution is non-binding, it illuminates the perspective of the European Parliament against such predictive policing technologies, and some critics observe it gives an indication on how the Parliament is likely to vote on the AI Act.[23] The opinion of the European Parliament relatively reflects verbatim the previously addressed weaknesses of the GDPR which can inevitably spill over into real world scenarios of victims of unregulated data usage and consequent discriminatory decisions based on predictive policing technologies. It stands to reason that artificial intelligence cannot predict with accuracy someone's propensity to commit a crime because 'data has both homogenous and heterogenous character'.[24]

Similarly, where automated processing is permitted under the exceptions, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

8. Conclusion

As can be seen by the predictive policing technologies, the ostensible capability to predict future criminal outcomes based on big data analytics can have an array of issues. From discriminatory outcomes, lack of regulatory data protections and criticism from the highest European authorities, ADM in the realm of predictive policing is faced with an abundance of challenges. According to the diaspora in the *Big Brother Watch*[25] case*,* there is a reported increasing trend for police forces in the UK to acquire, develop and operationally deploy technologies that are intrusive, untested and of questionable compatibility with fundamental rights. The crux of the issue is that whilst these technologies can have a positive impact on law enforcement procedures,

[21] ibid.
[22] ibid, para 8.
[23] Tetyana Krupiy, 'A Ban on Using Predictive Policing to Forecast Human Behaviour: A Step in the Right Direction' (*EU Law Enforcement: Central Point of Information, Research and Discussion,* October 2021) <https://eulawenforcement.com/?p=8102> accessed 11 February 2022.
[24] ibid.
[25] *Big Brother Watch & Ors v UK* App no.s 58170/13, 62322/14 and 24960/15.

there is simply not sufficient regulation under the GDPR for protection data subjects to justify the activity. To dichotomise by quoting a software developer who stated 'if I recognise patterns, I can look into the future, and when I can look into the future, I can shape the future'.[26] This can be read in both an optimistic or ominous tone, depending on how the future is perceived. With predictive policing ADM, yes there could be more people surveilled and a higher level of police protection, but there in turn could also be severe discrimination and data right infringements. Taking into account the previously outlined criteria for the GDPR to apply to ADM and predictive policing profiling, a regulatory mitigation should remove the lacuna permitted by the dilution of Article 22 and hopefully upcoming AI Act[27] will also impose tighter restrictions on such law enforcement tactics.

[26] Mareile Kaufmann, Simon Egbert and Matthias Leese, 'Predictive Policing and the Politics of Patterns' (2019) 59(3) The British Journal of Criminology, 674–692.
[27] Proposal for a Regulation of the European Parliament (EP) and Council (EC) Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021/0106 (COD).

WON'T SOMEBODY PLEASE THINK OF THE CHILDREN: ASSESSING THE GDPR'S ADEQUACY IN PROTECTING CHILDREN'S DATA

Daniel Mooney[28*]

Abstract

The right to privacy is a fundamental human right and its relevance has grown increasingly stronger in today's technology-driven world. The corresponding right to the protection of one's personal data has emerged as a key safeguard to people's privacy in cyberspace, where much of the online economy is powered by the harvesting and analysis of user data. These safeguards are especially important for children, who can be particularly vulnerable in the online world. The General Data Protection Regulation (GDPR) is the European Union's most important data protection legislation, with Article 8 being the key protection for children's data alongside other ancillary protections. While the GDPR's novel inclusion of specific rules for the protection of children's data is welcome, shortcomings and inconsistencies are present in the overall framework. This article aims to examine and analyse the GDPR's protections for children's data, seeking to illustrate areas where deficiencies are present. It will briefly consider the United States' COPPA regulations, with a view to identifying any lessons to be learned, before concluding by assessing whether the GDPR is adequate in protecting children's rights online.

[28*] Daniel Mooney LL.B. (NUI), is an LL.M. candidate in Trinity College Dublin specialising in intellectual property and information technology law. His current research focuses on European technology regulation on emerging artificial intelligence trends, with specific regard to synthetic media. His broader research interests include data protection, platform regulation, digital single market policy as well as Irish enforcement of civil judgment systems.

'*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.*'[29]

1. Introduction

The ever-increasing proliferation of technology, the pervasiveness of social media and the development of 'Big Data' have all posed challenges to fundamental rights. This is particularly the case with the rights of children, who are considered to be more vulnerable online especially in relation to consenting to service terms and manipulation of behaviour via algorithm.[30] Not to mention the issues around the use of children's data by large tech companies for marketing purposes and the rather troubling implications of such tracking.[31] This is all the more concerning, considering the growing numbers of young people who access the internet on a daily basis. UNICEF estimates that one in three internet users are people under 18 years of age,[32] with the majority of European children accessing the internet via smartphones and other devices daily.[33] With children making up a substantial demographic of internet users, it is absolutely essential that their rights and their data are protected. On the other hand, with the internet playing such a major role in the lives of children and young people, including increasingly in their social and educational development, it is equally vital that access to the benefits of the internet is maintained.

Both European policy statements and the GDPR itself make clear that children are deserving of particular protection under data protection law, in consideration of their unique circumstances and legal risks.[34] Indeed, the various competent authorities across the member states have made clear that violations of the child-consent principles will result in enforcement and substantial penalties.[35] However, in spite of this laudable aim, deficiencies remain in the GDPR's legislative framework which leave the protection of children's data somewhat inconsistent across the European Union. At its core, the GDPR acts to guarantee human rights in respect of privacy and data protection. This is equally the case for children, who are generally more vulnerable online in

[29] Recital 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 2016 L 119/1. (Herein, '**GDPR**').
[30] Thomas Anders, Using Choice Architecture to Counter Nudge Online' (2021) 39(12) Irish Law Times 173, 174.
[31] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U, *EU Kids Online 2020: Survey results from 19 countries* (EU Kids Online, 2020) 6.
[32] Sonia Livingstone, John Carr and Jasmina Byrne, *One in Three Internet Governance and Children's Rights. (*Global Commission on Internet Governance 2015) 3.
[33] Smahel et al. (n 31), 10.
[34] For instance, see Recital 38 (n 29).
[35] Up to 10% of Revenue – GDPR, Article 83.

any case. Thus, it is absolutely essential and pertinent to assess whether the GDPR is acting effectively as a safeguard to children's data and, by proxy, their human rights.

This essay aims to critically analyse the GDPR, seeking to answer the question as to whether or not the Regulation adequately protects children's rights. It will begin by briefly providing some background to children's data protection prior to the GDPR and will then move to an overview of the provisions contained within the Regulation. The focus will then move to consider the core issue of consent. It will be argued that the GDPR has a somewhat unsatisfactory approach to the issues arising from the digital age of consent as well as general concerns over the scope of the Article 8 requirements. The essay will also briefly consider requirements under Article 12 for transparency as well as minor ancillary provisions. The essay will then look at the level of protections afforded to children's data in the United States in contrast to those under GDPR, seeking to identify any lessons that can be learned. Finally, the essay will conclude by analysing the overall adequacy of the GDPR's protections for children's data, arguing in favour of more robust protections to enhance and guarantee the protection of children's rights to privacy.

2. Introduction and Pre-GDPR Background

Before exploring the myriad of protections and policy proposals around children's data protection, it is submitted that there is value in examining why children need specific safeguards under data protection regimes in the first place. Both scholars and data protection regulators are of the opinion that children merit specific and special protection under the law. For instance, the Irish Data Protection Commission has officially stated in its children's consent guidelines that '*For all users of online services, how personal data is processed, by whom and how this is used, is often complex and opaque. Children cannot be expected to manage this complexity themselves, nor ensure their rights are upheld.*[36] Children are inherently at a greater risk of manipulation online due to their lower developmental capacity, which means that they lack the ability to meaningfully consent to service terms and understand the ramifications of online activity.[37] They may, as a result, be more at risk to the potential for harmful outcomes from online engagements and may not fully appreciate the

[36] Data Protection Commission, *Fundamentals for a Child-Oriented Approach to Data Processing Draft Version* (Data Protection Commission, 2021) <https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf> accessed 24 November 2021.

[37] Beeban Kidron, 'Are Children More Than Clickbait in the 21st Century' (2018) 23(1) Communications Law 25, 27-28.

long-term impact of their actions.[38] In the world of 'big data', this can leave children at risk of giving away their data with no real comprehension as to the impact that this may have on them in future. This is particularly the case where the incentive for information society services is to collect as much data on children and young people as possible, given the fact that the youth advertising market alone is worth billions of dollars.[39] Thus, where children are at risk of the wholesale collection and exploitation of their data without their meaningful consent and, where the clear economic incentive is to continue this activity, regulatory intervention is needed to safeguard children and by extension the principle of informed consent. It is overwhelmingly clear that specific and special protection should be provided for children in relation to their data, in accordance with broader 'children's best interest' provisions under EU[40] and international law.[41] Although such policy objectives now seem necessary and obvious, children were not always recognised as needing any higher standards of safeguarding.

The GDPR's introduction of child-specific provisions was a novel development in data protection law.[42] Traditionally, children were considered indistinct in terms of data protection with the focus being on generalist protections for all natural persons. Indeed, prior to the enactment of the GDPR, children enjoyed no special protection in relation to their personal data and were treated in the same way as adults under both the Council of Europe's Convention 108 and the EU's Directive 95/46/EC.[43] This failure to distinguish between children and adults leads to a number of problems. For instance, regarding a digital age of consent, the old regime left the decision about whether to process children's data as a subjective assessment that had to be made by the data controller.[44] Both the Irish Data Protection Commissioner and the Article 29 Working Group advised that the decision would have to be made based on the child's maturity,[45] something which, it is submitted, is a very onerous task to place on would-be controllers. Another issue arose in relation to what legal instruments should govern children's consent to receipt of information society services i.e., was a Member State's contract law the governing law

[38] Laurence Steinberg, 'Risk Taking in Adolescence: New Perspectives from Brain and Behavioural Science' (2007) 16(2) Current Directions in Psychological Science 55.
[39] The rough estimate is $1.7bn. See Susan Raab, 'Protection of Children's Data and Where Reforms are Needed' (2021) 4(4) Data Protection and Privacy Journal 347.
[40] European Charter of Fundamental Rights [2012]OJ C 83, 30.3.2010, p. 396–396.
[41] UN Convention on the Rights of the Child, Ratified 20 November 1989, UNTS 1577.
[42] Tom Anders' Children and Data Protection' (2021) 39(17) Irish Law Times 250.
[43] Sonja Kress & Daniel Nagel, 'The GDPR and its Magic Spells Protecting Little Princes and Princesses. Special Regulations for the Protection of Children Within the GDPR' (2017) 18 Computer Law Review International 6.
[44] Lorraine McDermott, 'Too Much, Too Young": The Age of Consent On Social Networking Sites' (2011) 29(1) Irish Law Times 259.
[45] Article 29 Data Protection Working Party, 'Opinion 2/2009 on the protection of children's personal data' (European Commission, 2009).

for such digital consent. However, if that was in fact the case, could a person under 18 consent at all?[46] Overall, it can be easily appreciated that considerable uncertainty existed under the old Directive's regime with the approach to children's data protection being very much a case of 'seen and not heard'.[47] The failure to distinguish between children and adults, particularly in respect of consent to processing, was subject to much criticism and resulted in policymakers ensuring that the GDPR set out special protections for children's data.[48] What is clear from examining both the policy rationale and the background to the GDPR is that the Regulation aims to place the protection of children's data on a higher standard than adult's data processing, with the overall aim of safeguarding children. While the GDPR's novel inclusion of specific safeguards for children had the aim of harmonising and modernising the landscape for children's data processing, as will be seen, its effect has been mixed.

3. Article 8: Overview and Scope

Article 8 is the key provision of the GDPR when it comes to children's data and their rights. Acting as a qualification to the Article 6 consent requirements, Article 8 sets out the key provisions for the digital age of consent and the obligations on data controllers to get parental consent when the child is under that age.[49] Article 8 reads as follows:

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.[50]

At the core of Article 8 are the extra protections that are aimed at protecting children's rights with Recital 38 acting as a companion, setting out the ancillary reasoning and policy objectives.[51]

[46] Steinberg (n 38), 262.
[47] McDermott (n 44) 6.
[48] Kidron (n 37), 7.
[49] Eleni Kosta, 'Article 8: Conditions applicable to child's consent in relation to information society services' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 356.
[50] GDPR, Article 8.
[51] McDermott (n 44) 8.

Although its objectives of protecting children are broad, the scope of the article itself is somewhat narrow and straightforward.[52] As aforementioned, Article 8 applies to the conditions applicable to children's consent to their data being processed. The Article requires that where a child is under the age of digital consent, which is to be determined by Member State law, parental consent is required to process any data pertaining to that child user.[53] The age of digital consent, which is discussed substantially below, can be no lower than 13 years of age. Under the second paragraph of the article, the controller is under an obligation to make 'reasonable efforts' to verify the parental consent provided for those users who fall below the age of digital consent. These 'reasonable efforts' are not clarified by the GDPR and are left up to the discretion of companies.[54] Finally, Article 8 applies only to when information society services use consent as a lawful basis for which data is processed and does not apply to the other bases like legitimate interest etc.[55]

The scope of Article 8 is further narrowed to only include information society services that concern children specifically. The use of the words 'offered directly to a child', limits the applicability of the article to only those information society services that offer their services to children, meaning that services which make clear that their services are available only to those aged 18 and over will of course not be bound by the consent requirements.[56] The original proposals for reform from the Article 29 Working Party recommended that this provision be worded to be much broader in application to processing beyond that of information service societies although the Commission opted not to follow such proposals.[57] As such, only information society services, as defined by the GDPR[58] in reference to the Single Market Transparency Directive,[59] are captured by the provisions. This is relatively simple for specific scenarios and captures services like YouTube Kids which are very clearly marketed toward younger users. However, problems arise when it comes to services that are not directly aimed at

[52] Kosta (49), 356.
[53] GDPR, Article 8(1).
[54] Kidron (n 37).
[55] Lisa Atkinson, 'Interpreting the Child Provisions of the GDPR' (2018) 23(1) Communications Law 31.
[56] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (2020) 25. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> Accessed 14 November 2021.
[57] Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals' (European Commission, 2012) 13 <https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2012/wp191_en.pdf> accessed 16 November 2021.
[58] GDPR Article 4(25).
[59] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015.

children but which potentially have a large youth userbase. Services which have a mixed user base or are geared towards a general audience pose problems for the Article 8 consent regime.[60] Difficulty arises as there is no guidance on how such services should be dealt with. The Bavarian Data Protection Agency has said such services should be covered but that view is not universal.[61] It is submitted that the scope of Article 8 in this case is relatively narrow, leaving many instances of children's data being processed offline and online, essentially untouched by the higher standard consent provisions. It is now proposed to move on to examine the provisions in respect of the digital age of consent, an area which poses further problems for the consistency of the Regulations implementation.

3.1. The Digital Age of Consent – Variance and Vagary

In its early drafts, the GDPR defined a child as anyone under the age of 18 and their protections were contained within Article 7 as a rule that broadly limited children's consent to parental authorisation.[62] As is clear from the wording of Article 8, this was abandoned by the Commission during the drafting process. In its stead, the GDPR creates a European 'digital age of consent', granting Member States the broad right to set a digital age of consent of anywhere between 16 years of age and 13 years of age, although no lower nor higher.[63] Prior to the GDPR, the digital age of consent varied widely and was left up to the discretion of the Member States as the original Data Protection Directive was silent on the matter.[64]

Despite the GDPR's aim of harmonising the approach to the digital age of consent, the framework has in fact altered little in respect of the varying ages across Member States.[65] Currently, the digital age of consent continues to vary widely between various Member States with several opting for the minimum and maximum ages respectively. For example, Ireland,[66] the Netherlands and Poland have a digital age of consent set at 16 years while Estonia, Sweden and Portugal have opted for 13 years.[67]

The decision to select a lower age is more-in-line with current practice amongst platforms and is

[60] Kidron (n 37), 24.
[61] Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15' (BayLDA, 20 January 2017) <https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf> accessed 26 November 2021.
[62] Kosta (49), 358.
[63] Denis Kelleher & Karen Murray, *EU Data Protection Law* (1st edn, Bloomsbury 2018) 160.
[64] For instance, in the UK the digital age of consent was 12 while in Spain it was 14.
[65] ibid.
[66] See generally Data Protection Act 2018 s31.
[67] For further on these jurisdictions, see Eva Lievens and Ingrida Milkaite, 'Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU' (Better Internet for Kids, 1 July 2019) accessed 29 November 2021 <https://www.betterinternetforkids.eu/enGB/practice/awareness/article?id=3017751>

justified on grounds of allowing children greater access to online space.[68] Persano, for instance, also makes the argument that a lower age of digital consent is more beneficial as it indirectly increases responsibility on platforms to make better efforts at protecting younger children.[69] It is respectfully argued that this does not necessarily follow. Indeed, a lower age merely allows for less protections for children aged 14 and over with dubious benefits for younger children. While one could object to a 16-year-old requiring their parent's consent on expression grounds, it is submitted that protection is preferable in situations where young users can be exposed to harmful content or indeed the manipulation of their data.[70] Overall, these arguments have created a divergence of opinion and as a result the digital age of consent varies considerably between the Member States.

The lack of uniformity among Member States is problematic, especially for information society services that provide services internationally. Indeed, this has the effect of splintering the internal market and increasing uncertainty for those providing cross-border services.[71] Naturally, the question arises; at what age can service providers process data on a standard consent basis in the EU? The core issue is that the answer to this question will depend on where the service provider is operating and processing the data.[72] Unfortunately, this issue and other pertaining to children's consent have yet to be considered by the Court of Justice of the European Union (CJEU) and no real guidance can be gleaned from case law in relation to the inconsistency of treatment and which standard should be applied.[73] Another problem that arises with respect to the varying age across the Union, is that it leaves some children protected to 16 with others only until 13. Kress and Nagle note that this waters down the level of protections afforded under Article 8.[74] One of the core issues around setting the digital age of consent is establishing how mature and able a child is to consent to their data being stored, processed and used for targeting or profiling purposes. Establishing this is inherently difficult and problematic.[75] Children mature at different rates and each child will be unique in how comprehensively they will understand what

[68] Kidron (n 37), 40-41.
[69] Federica Persano, 'GDPR and Children's Rights in EU Data Protection Law' (2020) European Journal of Privacy Law and Technologies 32, 42.
[70] Simone Van Der Hof, 'I Agree or do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34(2) Wisconsin International Law Journal 416, 419.
[71] Milda Macenaite & Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 127.
[72] Sonia Livingstone, 'Children: A Special Case for Privacy?' (2018) 46 Intermedia 18, 21.
[73] ibid, 19.
[74] McDermott (n 44) 16.
[75] Liliana Pasquale, Paola Zippo, Cliona Curley, Brian O'Neill, and Marina Mongiello, *Digital Age of Consent and Age Verification: Can They Protect Children?* (LERO, 2021) Accessed on 29 November 2021 <https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1104&context=aaschmedart>.

information they are exchanging for access to information society services.[76] This of course causes problems when attempting to set a definitive age as interpretations will vary. Despite this, it is important that the approach is consistent as, without consistency, regulation and compliance are made more difficult. Inconsistency and variance unfortunately lead to some children being more protected than others.[77]

Overall, there are fundamental criticisms of the consent regime as a whole. For instance, Van Der Hof and Lievens argue that children and parental consent is actually an ineffective means of data protection as it leads to the illusion of protection.[78] They argue rather, that the best means of protection of children's data lies in privacy-by-design approaches and by ensuring that data controllers place emphasis on a child-centred process, granting control and autonomy to children over their own data.[79] Certainly, it can be argued that the risk of ill-informed consent can pose a risk to both children and data controllers.[80] In this vein, there have been arguments that information society services should avoid using consent as grounds to process children's data.[81] The UK's Information Commissioner's Office has also encouraged information society services to avoid consent as a ground for processing children's data, instead utilising the legitimate interests ground as it requires a fair and proportionate consideration of whether such data is needed.[82] However, legitimate interest justifications, although simpler from a controller point-of-view, may not actually protect children any more than consent-based processing.[83] Overall, broader issues also arise in relation to data gathering notices and consent more broadly, for instance through inadequate cookie notices, which may have an end result of affecting children through the choices made by their parents.[84]

3.2. Age and Consent Verification

Age verification poses further difficulties. One can very easily imagine a scenario where a child is

[76] ibid, 4.
[77] ibid, 421.
[78] Simone Van Der Hof and Eva Lievens, 'The Importance of Privacy By Design and Data Protection Impact Assessments In Strengthening Protection of Children's Personal Data Under The GDPR' (2018) 23(1) Communications Law 33, at 37.
[79] ibid, 43.
[80] For instance, the risk of large administrative fines.
[81] Christopher Kuner, *European data protection Law: corporate compliance and regulation* (2nd edn, Oxford University Press 2007) 312.
[82] UK Information Commissioner's Office, *Consultation GDPR Consent Guidance*, (UK ICO, March 2017) 27. <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 24 November 2021.
[83] Virginia M Talley, 'Major Flaws in Minor Laws: Improving Data Privacy Rights and Protection for Children Under the GDPR' (2020) 30(1) Indiana International and Comparative Law Review 127, 150.
[84] Anders (n 30).

asked to provide a form of verification by email and simply selects a false email address in which they themselves can provide the consent posing as their parents, essentially negating the verification process. Thus, it is necessary for the controllers to ensure that the methods selected for verification are fit for purpose and 'child-proof.' One of the core issues with verification arises in relation to how such parental consent can be verified. As mentioned in the initial overview of the scope of Article 8, under paragraph 2 the data controller is obliged to make reasonable efforts to verify the consent made on the child's behalf by their parent or guardian. The GDPR does not define what 'reasonable efforts' actually entails and the guidance on the matter is unfortunately not much clearer, simply stating that 'reasonable efforts' will depend on each individual organisation's situation.[85]

One such solution has been the concept of digital IDs, such as the ones currently being trialled in Estonia although concerns around such methods exist.[86] Others, which mirror consent verification methods in America, include employing systems such as 'email+', freephone verification lines and credit card-based authentication.[87] While methods vary across the industry, it is argued that the lack of guidance and specific rules within the GDPR leave verification protections very much the preserve of the individual organisation, thereby creating disparity and confusion both for controllers and child-subjects alike.[88]

While more technological solutions can help to increase the accuracy and efficacy of verification, it is submitted that there is a risk of going too far in this respect. One could easily envisage a situation where controllers end up requesting and processing far more data, in particular sensitive data like credit card or even biometric data, in order to merely verify consent. Rather, efforts should be made to promote notice and awareness for parents of users under the digital age of consent. In essence, this would involve making parents aware of the data collection and processing activities thereby encouraging informed consent instead of complicated verification requirements that result in uninformed parents granting wholesale consent to processing anyway.[89]

3.3. Consent Provisions – Adequate Protection?

[85] Kidron (n 37), 41.
[86] Jake Maxwell Watts, 'One Country's Uber-Convenient, Incredibly Invasive Digital ID System' *The Wall Street Journal* (New York, 9 May 2019).
[87] For further, see Part IV discussion below.
[88] EDPB guidelines have little to say about verification. EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679* (EDPB, 4 May 2020) 25.
[89] Kuner (n 81), 38.

Regarding consent and the protections contained in Article 8, it is argued that the GDPR is not adequate in safeguarding children's data. While Article 8 is certainly an improvement on the previous lack of any child-specific provisions, its effectiveness is beset by fundamental issues which hamper its overall impact. The lack of clarity as to what kind of information society services fall within its scope and its limiting to only those services which directly target children, leave many children vulnerable in online environments in which they participate. It is submitted that more clarity in what services can and should be caught by Article 8 would be very welcome. This is likely to come from the relevant supervisory authorities or through the EDPB, although regardless a consistent and cross-border approach is vital.

The GDPR's failure to harmonise the digital age of consent has also left the regulatory situation somewhat unclear and ineffective, leaving a situation where some children are protected more than others. This also poses problems for the digital single market's integrity and complicates the situation for international service operators. Finally, verification remains solely the domain of the information society service that the child is using, leaving protection unsatisfactory and without statutory backing. Overall, it is posited, the protections as they currently stand are inadequate and do not provide for the kind of informed consent that the principle-based approach envisages.

4. Transparency and Ancillary Protections

While the provisions around consent under Article 8 make up the bulk of child-specific protections in the GDPR, there are some other important sections that should also be considered. One area where the GDPR also aims to protect children is through transparency requirements, which although in a general sense make reference to children as an audience. Under Article 12(1), controllers and processors are required to ensure that information provided for data subjects in clear, intelligible and in plain language, 'in particular for any information addressed specifically to a child.'[90]

Children of course also benefit from general transparency requirements, including for example prevention of nudge behaviours[91] through the GDPR's prevention of automatic tick-boxes.[92] [93] In terms of improvement, there is a variety of suggestions to improve transparency. These

[90] GDPR Article 12(1).
[91] For further, see Anders (n 30).
[92] C-673/17 *Planet49* [2017] ECLI:EU:C:2019:801.
[93] Case C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* [2019] ECLI:EU:C:2020:90.

include child-friendly ways of communication such as icons, graphics, videos or chatbots.[94] These can also prove helpful in removing overly complex legal language which serves to confuse and potentially manipulate children and their parents, having the overall effect of making consent illusory.[95]

A lack of clarity also exists in relation to Article 22, in particular with regard to the exact rules to be applied to children in automated decision-making.[96] Finally, indirect protections can also be found under Article 57 which requires the various supervisory authorities to promote education initiatives on such issues[97] as well as to inform controllers and processors of their obligations under the Regulation generally.[98] In many ways, the transparency requirements along with the ancillary provisions provide addendums to the Article 8 protections. While strong in principle, it is submitted that further soft law intervention as envisaged by Article 57 is required to ensure the application of such protection in practice.

5. Learning from Experience – Lessons from COPPA

It can certainly be argued that the GDPR continues to be the world's leading legal standard when it comes to the protection of personal data. In many ways, this is due to what Bradford describes as 'the Brussels effect'.[99] Regardless however, of the GDPR's truly global footprint, there are still lessons that can be learned from other jurisdictions in respect of data protection. The safeguarding of children's data is one of these areas where comparative analysis can prove informative. Somewhat unusually, it is in the United States in which a long-standing and influential data protection regime concerning children can be found. Indeed, Macenaite and Kosta note that, in many ways, the GDPR's child protection provisions take inspiration from those that have been in place in the United States for a number of years.[100]

The primary federal legislative instrument for the US is the Children's Online Privacy Protection Act (COPPA).[101] COPPA, which dates from 1998, sets out substantial provisions dealing with the ability of children to consent to the use of online services. COPPA sets the digital age of

[94] Ingrid Milkaite & Eva Liebens, 'Child-friendly transparency of data processing in the EU: from legal requirements to platform policies' (2019) 14(1) Journal of Children & Media 5, 19.
[95] ibid, 22.
[96] Pasquale et al. (n 75), 47.
[97] GDPR, Article 57(1)(b).
[98] ibid, (1)(d).
[99] See generally, Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).
[100] Stuart Cobb, 'It's COPPA-cated: Protecting Children's Privacy in the Age of YouTube' (2021) 58(4) Houston Law Review 4.
[101] Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–650 (USA).

consent at 13 years of age and requires parental consent for any child falling below that age.[102] The Act's definition of children's personal information is expansive[103] and it further requires online service operators to have a COPPA compliant plan in place to provide notice to parents and obtain consent.[104] It is aimed at services 'directed at children' which the FTC considers to include sites with characteristics like child-orientated content, young models etc.[105] The issue of general audience services also arises in a US context. COPPA applies to services directly aimed towards children but also applies to sites which are general in nature but have significant youth userbases, however this is only where actual knowledge is held.[106] This means that services will oftentimes have minimum user ages set at 13 and any under-aged users that attempt to register will be blocked although some sites simply avoid the compliance obligations by avoiding actual knowledge.[107] This is a weakness present in both the US framework and the GDPR.

One of the marked differences between COPPA and Article 8 of the GDPR is the requirement for parental consent being more absolute in the US. As noted above, Article 8 requires parental consent to be given or authorised i.e., the parent may authorise the child to give consent. COPPA is more specific in its rules and requires that organisations get verifiable consent from parents in advance, subject to limited exceptions.[108] Verification methods are not explicitly set out in COPPA but the Act states that 'reasonable efforts' must be made by operators to obtain verified parental consent with consideration to the available technologies at the time.[109]

While the GDPR does not define what is meant by 'reasonable efforts' in Article 8, COPPA could offer some guidance as to what such efforts might look like and may provide assistance to European policymakers in what approaches can work to verify parental consent. For instance, the Federal Trade Commission recommends, through its COPPA guidance, credit or debit card identification methods, 'email+'[110] and others to ensure that parental consent is genuine.[111] This is an area where the GDPR and indeed supervisory authorities should look to in informing their own approach to ensuring compliance and guiding industry standards. It is submitted that the

[102] ibid.
[103] Talley (n 83), 147.
[104] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2(A)(1)(a) (2013) (USA).
[105] Livingstone (n 72).
[106] ibid, 146.
[107] ibid.
[108] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2013) (USA).
[109] ibid, ss 316.4.
[110] 'Email+' is a verification method that involves a parental email address and one other form, normally postal or telephonic communication of consent.
[111] Jeremy Meisinger, 'Cybersecurity 2019 — The Year in Preview: COPPA, the GDPR, and Protecting Children's Data' (Foley Hoag LLP, 2019) <https://www.jdsupra.com/legalnews/cybersecurity-2019-the-year-in-preview49904/ [https://perma.cc/R36U-M2PP].> accessed 27 November 2021.

Article 8 allowance for parental authorisation as well as consent gives more flexibility to information society services although at the expense of more stringent verification of parental consent. It is further submitted that the GDPR should arguably not 'straightjacket' what kind of methods should be used to verify consent and indeed COPPA can offer some useful possibilities when designing soft-law based frameworks for ensuring compliance with Article 8 requirements.

It is submitted that the United States takes a somewhat more paternalistic approach to children's consent and this can be observed from the numerous provisions relating to parental consent within COPPA. As mentioned above, COPPA has already informed many aspects of the GDPR's child consent protections through its impact on policymakers.[112] While far from perfect, COPPA offers guidance on how European data regulators should interpret provisions and can inform soft law initiatives, for instance mandatory codes of conduct, going forward.

6. Conclusion

In conclusion, it is clear that the GDPR has marked an improvement on the previous regime and its policy objectives are to be lauded. However, while its intentions are good, there are a number of shortcomings within the legislative framework. Assessing adequacy requires a nuanced approach. In particular, it is vital to bear in mind the delicate balancing act that must be performed in order to allow children and young people access online spaces in a safe way without placing unrealistic burdens on providers. While it can be said that the GDPR overall provides general protection, that protection is somewhat piecemeal and even illusory at times. It is submitted that these fundamental issues mean that the GDPR does not adequately protect children. Protections and safeguards are provided in respect of children's consent but this presupposes that consent is the best way to implement data protection. Indeed, as has been discussed above, consent as a basis for processing has been subject to criticism due to its in-practice weaknesses. Furthermore, shortcomings in the scope of Article 8 limit the GDPR's applicability, leaving children with uncertain protections on platforms for general audiences. The lack of guidance in respect of verification methods means that information society services are left to self-regulate age verification and that parental verification is not a guaranteed way to ensure compliance.

The failure of the GDPR to ensure a harmonised approach regarding the digital age of consent is unfortunate and has, in essence, simply replicated the pre-GDPR problem of inconsistency in

[112] Lievens and Milkaite (n 67).

the age of consent. While the effects of such variance on the internal market have yet to be seen definitively, the inconsistency creates confusion for online providers and fails to ensure adequate protection across all Member States. While transparency is promoted, there needs to be more intervention and guidance to ensure that it is truly transparent to both children and their parents to ensure that informed consent is not rendered illusory. The US' COPPA legislation and experience can provide guidance to European policy-makers in creating codes of conduct and other initiatives to strengthen the existing system.

Overall, the GDPR's protections are inadequate but that is not to say that they are wholly non-functional. Indeed, the GDPR does protect children's rights but it does not yet go far enough. At its very core, the protection of children's data online is a human rights issue. Children are particularly vulnerable to having their right to privacy and the protection of their data undermined through flaws in the statutory protections. Remedying these issues should be a priority for supervisory authorities and for policy-makers. It is submitted that the best way of tackling the shortcomings that exist would be through a mandatory code of conduct, clarifying how services can protect children and guarantee consent while also working toward a harmonised approach toward a European digital age of consent. With the intervention of supervisory authorities and co-regulatory solutions, the GDPR can achieve far greater protections for children and their data while ensuring their safe access to the digital world. Ultimately, through these actions, the GDPR can act as a fundamental guarantee of children's rights in cyberspace.

ARTIFICIAL INTELLIGENCE, ALGORITHMS AND THE FREEDOM OF EXPRESSION: TOWARDS THE DIGITAL SERVICES ACT AND BEYOND

Tea Mustać[113*]

Abstract

Algorithms are increasingly used by private companies to spot and potentially remove unlawful content as well as to sort the content available to best fit the users' needs. These developments have confronted us not only with unprecedented possibilities for open, public discussion but also with the potential deterrence of free expression. Furthermore, they have faced us with some difficult questions - such as defining hate speech or drawing the line between what is permissible and what is intolerable - that need to be answered in order to effectively protect the developed standards of speech protection. The focus of this paper is the intricate interplay between artificial intelligence, namely algorithms as its subcategory, and the freedom of expression as it is protected on the territory of the European Union. This paper aims to provide a thorough examination of the current legislation and the newly proposed regulation at the EU level in order to determine the impact of algorithmic content moderation and curation on the existing legal regime. Lastly, this paper will present potential changes that would strengthen the protection of freedom of expression online and level out the increasingly distorted playing field among various private and public actors.

[113*] Tea Mustać is a recent law graduate and former ELSA member from the Faculty of law in Rijeka (Croatia), with a keen interest in regulating the use of artificial intelligence in our everyday lives. Currently, she is working as a research associate in the field of data protection at the Spirit Legal law firm in Leipzig. This article was written during her one-year Erasmus+ exchange at the Karls-Franzens-Universität in Graz (Austria).

1. Introduction

The boundaries of free expression are increasingly determined by the Internet's new 'governors', commonly referred to as platform providers.[114] Governments have effectively transferred a part of their responsibility for protecting free speech to these providers, pressuring them to police unlawful content, and imposing substantial financial sanctions for failure to do so. [115] This pressure, combined with incomprehensible amounts of content generated every second,[116] forces platforms to heavily rely on algorithms that have come to determine the content users are exposed to.[117] The algorithms search websites for spam and viruses, copyright infringements, and pornography, while the indecent, objectionable, or too controversial is being scrubbed off.[118] However, these automated processes are not yet sophisticated enough to deal with the many challenges of content evaluation, such as its dependence on the constantly changing political, sociological, and personal context, or the necessary interpretation of the creator's intent.[119] Consequently, there is a high chance of misidentifying content as violating platform rules and regulations, thus raising freedom-of-expression concerns.

This paper aims to examine the legal impacts of the use of algorithms online on the right to freedom of expression, with the goal of determining the reason for society becoming dependent on data-driven processes when protecting this fundamental human freedom. Then, after providing a general overview of the challenges arising from this dependence, the paper will analyse the current EU regulation and the recently proposed Digital Services Act. The main hypothesis is that current and the newly proposed regulation cause a general tendency towards preventive over-blocking. It is argued that governments have tried to absolve themselves of both the financial and overall responsibility burden to protect the freedom of expression. Consequently, suggestions, recommendations, and amendments will be presented that would

[114] Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', [2017] UC Davis Law Review, Yale Law School, Public Law Research Paper No. 615, 1187-1193, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939> accessed 21 September 2022.
[115] Article 19 and Privacy International, 'Privacy and Freedom of Expression in the Age of Artificial Intelligence' [2018] 14 <https://www.article19.org/wp-content/uploads/> accessed 21 September 2022.
[116] See, for example, Evangelos Banos et al., 'PersoNews: A Personalized News Reader Enhanced by Machine Learning and Semantic Filtering' [2006] Conference: On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, OTM Confederated International Conferences, p.975, <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2101&rep=rep1&type=pdf> accessed 21 September 2022.
[117] Banos et al. (n 116), 975.
[118] Tarleton Gillespie, 'The relevance of algorithms, Media technologies: Essays on communication, materiality, and society' [2014] MIT Press, 6. <https://governingalgorithms.org/wp-content/uploads/2013/05/1-paper-gillespie.pdf> accessed 21 September 2022.
[119] Gillespie (n 118), 6.

retrieve some of the lost powers and responsibilities of the EU Member States ('the States'), strengthen the multistakeholder approach to speech governance, and enhance the protection of the freedom of expression.

2. The Basics

2.1. Freedom of Expression (and the Internet)

For the sake of simplicity, this article will focus on the protection of freedom of expression provided by Article 10 of the European Convention on Human Rights ('the Convention') and the following jurisprudence of the European Court of Human Rights ('the Court'), which is relevant and valid on the whole territory of the European Union through Article 52(3) of the Charter of Fundamental Rights of the European Union.[120] In that sense, it is important to emphasise that the Convention protects not only inoffensive and favourable information or ideas, but also those that 'offend, shock, or disturb'.[121] As Oscar Wilde once said 'An idea that is not dangerous is unworthy of being called an idea at all.', and censoring such ideas leads us towards a more restrained, autocratic society.[122] Furthermore, in addition to refraining from interfering with the right to freedom of expression, States also have the positive obligation to ensure that private individuals can effectively participate and exercise this right.[123] On the other hand, balance must be struck with other fundamental rights, and freedom of expression cannot be exercised at the expense of human dignity or in such a way as to constitute illegal behaviour.[124] As far as the Internet is concerned, *the rules of the game have to be adapted to this new environment and its inherent features. The amount of user-generated content uploaded provides an 'unprecedented platform for public discourse'*.[125] However, a growing amount of content in general also implies a growing amount of unlawful speech within it,[126] and such content can now be disseminated instantaneously,

[120] Article 52(3) of the Charter of Fundamental Rights of the European Union [2012] *OJ C 326/391*.
[121] European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights, §9.
[122] James Fieser, 'CENSORSHIP, From Moral Issues that Divide Us' [2021] <https://www.utm.edu/staff/jfieser/class/160/4-censorship.htm> accessed 21 September 2022.
[123] Dink v Turkey, App no 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (ECtHR, 14 September 2010) § 137 and Khadija Ismayilova v. Azerbaijan, App no 65286/13 and 57270/14 (ECtHR, 10 January 2019) § 158.
[124] For more, see Paul Sturges, 'Limits to Freedom of Expression? Considerations Arising from the Danish Cartoons Affair' [2006] IFLA Journal, 32, 181-188, <https://www.ifla.org/wp-content/uploads/> accessed 21 September 2022.
[125] Delfi AS v Estonia, App no 64569/09 (ECtHR, 16 June 2015) §110.
[126] Michele Finck, 'Artificial Intelligence and Online Hate Speech' [2019] Centre on Regulation in Europe (CERRE) 4, <https://cerre.eu/wp-content/uploads/2020/05/CERRE_Hate-Speech-and-AI_IssuePaper.pdf> accessed 21 September 2022; European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights, Freedom of Expression §538, 611.

worldwide, with the possibility of remaining permanently accessible online.[127] Unlike shocking or unpopular speech, unlawful speech (such as hate speech or the dissemination of false information) is not protected by freedom of expression and the States must do everything in their power to fight against it.[128] However, this has proven to be quite a task.

2.2. Platform Providers[129]

The current freedom of expression regime is shaped by relations and power struggles between various actors,[130] with private companies playing a major role since only they have the possibility to actually police against unlawful content.[131] However, these platforms are now imposing a set of values of their own, thus rapidly becoming 'a kind of sovereigns governing the behaviour of populations of end-users'[132] But what to make of these new rulers who are evidently playing a big role in people's everyday lives? Who governs them?

The companies being discussed are most often referred to as platform providers or platform operators,[133] since they provide a platform for all types of content (e.g. Instagram where users can post pictures, videos, audios, usually accompanied by textual descriptions), making it accessible to the public. These providers, as opposed to traditional media, do not edit the posted content and allow anyone to post, their obligation of impartiality is still not a legal one, and they operate with the sole goal of maximizing profit and engagement.[134] However, despite their private character, because of their role in facilitating public discussion they should bear at least part of the responsibility for the available content.

In the European Union, platform providers are still mostly governed by the e-Commerce directive,[135] which provides definitions incapable of encompassing the most popular and, when it

[127] Delfi AS v Estonia (n 129) §110.
[128] European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights, Freedom of Expression, §614.
[129] The terms platform providers, platform operators, platforms, and service providers, will be used interchangeably throughout the paper and refer to the same kind of actors as described in this Chapter.
[130] Balkin (n 114), 1.
[131] Article 19 and Privacy International, 'Privacy and Freedom of Expression in the Age of Artificial Intelligence' (n 115) 14.
[132] Balkin (n 114), 36.
[133] See, for example, Judit Bayer, 'Between Anarchy and Censorship Public discourse and the duties of social media, CEPS Paper in Liberty and Security in Europe' [2019], 2 <https://www.ceps.eu/wp-content/uploads/2019/05/LSE2019-03_Between-Anarchy-and-Censorship.pdf> accessed 21 September 2022.
[134] Bayer (n 133), 8-9.
[135] 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') [2000] OJ L 178/1.

comes to the freedom of speech, most problematic social media platforms.[136] Therefore, many authors have been suggesting a change of the definition[137] and it appears that they have been heard. The proposal for the new Digital Services Act ('DSA')[138] gives new definitions, which cover most service providers present nowadays.[139] The Regulation is, however, still not adopted and some of the changes it brings to fore are long overdue considering the impact on the public discourse some of these service providers have.[140] It remains to be seen how long the changes brought about by the DSA stay relevant, and one can only hope that they do not already become insufficient by the time the regulation is enforced.

2.3. Artificial Intelligence and Algorithms

The discussed platform providers increasingly rely on algorithms to oversee the content being uploaded. These 'encoded procedures'[141] help navigate the sea of information available online,[142] determining the information that is consumed by users through content moderation and content curation.[143] While the former is used to proactively detect problematic content, and decide to remove, label, demote, or prioritise it,[144] the latter is here to help users determine what is 'relevant' through various recommendation algorithms.[145] Both functions present themselves as handy tools. Content moderation protects users from unlawful and undesired content, while curation relieves them of the tedious task of searching for the 'relevant' in the vast sea of published information.[146] It is very convenient having someone (or something) find all the needles you lost (and keep losing) in the haystack. However, in the last few years, a point of dependence on this luxury was reached, and one can say we began living in an 'algorithmic

[136] See, for example Bayer (n 133), 2. Article 2(a) of the 'Directive on electronic commerce' (n 135) and Article 1(2) of the Directive 98/48/EC amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 217/18. For a more detailed analysis, see Chapter 4.1.
[137] See, for example Bayer (n 133), 2.
[138] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 2020.
[139] Alexander Peukert et al., 'European Copyright Society – Comment on Copyright and the Digital Services Act Proposal' [2022] IIC - International Review of Intellectual Property and Competition Law volume 53, 358, p.366-367 <https://link.springer.com/article/10.1007/s40319-022-01154-1> accessed 21 September 2022.
[140] See, for example, Balkin (n 114), 53.
[141] Gillespie (n 118), 1.
[142] ibid 1, 17.
[143] Emma Llansó et al., Artificial Intelligence, Content Moderation, and Freedom of Expression [2020] Transatlantic Working Group p.14-15, 18 <https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf.> accessed 23 September 2022.
[144] See, for example, Barbora Bukovska, 'Spotlight on Artificial Intelligence and Freedom of Expression #SAIFE' [2020] Office of the OSCE Representative on Freedom of the Media (RFoM), 32-34 <https://www.osce.org/files/f/documents/9/f/456319_0.pdf> accessed 21 September 2022.
[145] Llansó et al (n 143), 14.
[146] ibid.

society'. A society 'organised around social and economic decisions made by algorithms, robots, and Al agents'.[147]

3. Where it All 'Goes South'

3.1. Governmental Pressure and Handling the Information Overload

The States have the responsibility to protect free speech, but also to protect individuals from unlawful speech.[148] However, they often do not have the ability or the resources to prevent unlawful content from being posted or remove it once it is online. Consequently, they adopt regulations with the effect of pressuring the service providers into patrolling for harmful and unlawful content for them.[149] On the other hand, incomprehensible amounts of content are generated every moment with nearly 66,000 photos on Instagram, 1.7 million posts shared on Facebook, 347,000 tweets on Twitter, and 5.9 million search queries on Google appearing each minute.[150] These amounts *are far beyond what any human can supervise, including what technological giants are feasible of processing without relying on algorithmic assistance and* often erring on the side of caution due to very high fines for failed compliance imposed by the States.[151] It seems that giving each and every person a megaphone might not be such a good idea, and it is the algorithms protecting people from what they do not wish to see or hear. However, algorithms have their own issues and blindly relying on their assistance can create an even worse situation than it was to begin with.

3.2. Challenges

After identifying the 'main suspects', algorithms, the consequences of their technological deficiencies can be discussed. Hate speech will be taken as an example since it is central to the current public debate, but similar conclusions could be drawn for any other kind of unlawful speech for which States have so far provided only vague, non-universal, or too narrow definitions.[152]

---

[147] Jack. M. Balkin, 'The Three Laws of Robotics in the Age of Big Data' [2017] Ohio State Law Journal, Vol. 78, 1217, p.1219 <https://digitalcommons.law.yale.edu/> accessed 21 September 2022.
[148] European Court of Human Rights, Guide on Article 10 of the European Convention on Human Rights, Freedom of Expression, §614.
[149] Article 19 and Privacy International, 'Privacy and Freedom of Expression in the Age of Artificial Intelligence' (n 115).
[150] DOMO, Data Never Sleeps 10.0 <https://www.domo.com/data-never-sleeps> accessed 24 September 2022.
[151] Llansó et al (n 143), 9; Article 19 and Privacy International, 'Privacy and Freedom of Expression in the Age of Artificial Intelligence' (n 115).
[152] See, for example, Finck (n 126), 4.

3.2.1. Artificial intelligence is not that intelligent

First, the States must decide what kind of speech cannot be tolerated. However, even with clear-cut criteria, algorithms could not handle human malevolence, ill-intent, jokes, or satire.[153] The most notorious example of how easy it is to trick an algorithm is the use of the word 'love'. This word alone can make speech that would otherwise be labelled offensive pass undetected.[154] Labelling the word love as indicating hate speech is of course out of the question, instead an interpretation of context, culture, political climate, social norms, and the intention of the speaker should be conducted. This is something humans do naturally, and this is precisely the reason it cannot (at least yet) be encoded into an algorithm.[155] The second major issue is that algorithms support biases by, for instance, making discriminatory decisions.[156] An algorithmic model for making admission decisions based on predictions of collegiate success could falsely discard qualified black applicants more often than qualified white applicants, simply because the engineer did not program the algorithm to equalise the false-positive rates between the two groups.[157] On the other hand, algorithms are yet incapable of recognizing their biases and therefore also fixing them, unless the programmers specifically ask them to do so and explain how exactly to do that. Lastly, it is worth noting that algorithms are not the only ones struggling with human intentions. If the practice of the ECHR is observed, a number of decisions dealing with this freedom and made by a very tight margin of votes can be found. For instance, in the case of Vereinigung Bildender Künstler v. Austria, [158] the ECHR has decided, by four votes to three, that there has been a violation of the freedom of expression. The case concerned a painting showing prominent Austrian figures in extremely indecent poses. It was banned from further exhibitions by the Austrian courts and the ECHR held that this measure violated Article 10. If the most esteemed judges of Europe can barely agree on such matters, how can one expect the algorithms to 'correctly' make these decisions? Respecting the fact that some situations are less complex and some violations more obvious, it is still a question of human intention that needs to be

[153] ibid, 6.
[154] Tommi Gröndahl et al, 'All You Need is « Love »: Evading Hate Speech Detection' [2018] 7-8 <https://arxiv.org/pdf/1808.09115.pdf> accessed 22 September 2022.
[155] Karen Hao, 'Giving algorithms a sense of uncertainty could make them more ethical' [2019] MIT Technology Review <https://www.technologyreview.com/2019/01/18/103546/giving-algorithms-a-sense-of-uncertainty-could-make-them-more-ethical/> accessed 23 September 2022.
[156] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' [2017] 413 <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf> accessed 21 September 2022.
[157] Michael Kearns and Aaron Roth, *The Ethical Algorithm The Science of Socially Aware Algorithm Design* (Oxford University Press, 2020) 10.
[158] Vereinigung Bildender Künstler v. Austria, App no 68354/01 (ECtHR, 25 January 2007).

interpreted and artificial intelligence is simply not yet intelligent enough to make such judgements.

3.2.2. Explain yourself

The regulation of the freedom of expression by private actors falls short of satisfying many legal safeguards.[159] One major issue in this regard is that there is no legal obligation of transparency.[160] This is especially the case, since many of the algorithms concerned are considered trade secrets.[161] However, even if this was not the case, algorithmic systems are very complex to explain and grasp.[162] Complete transparency is simply impossible due to the complex processes underlying an algorithmic decision.[163] On the other hand, although in human-made decisions complete transparency is also unfeasible since people are not aware of all factors influencing their decision, people still can explain those decisions. Conversely, algorithms are incapable of providing explanations other than general, non-specific ones, such as 'the content violates the Community Guidelines'.[164] To tackle this problem, various attempts have been made to envision satisfactory explanations for discontented users, but these are mainly exploratory or pedagogical in nature.[165] While in the former, users would be free to explore what results would emerge if they changed some features of their profiles, in the latter, providers could explain the underlying logic of the decision-making criteria and process without giving away the actual algorithm. However, this is far from the explanation average users would seek when they think their post was wrongfully taken down or that they are being discriminated against by the recommendation system.[166] This closely relates to the way this issue was tackled in the General Data Protection Regulation ('GDPR'),[167] where in Article 15 (1)(h) the users are granted the right to access meaningful information about the criteria and the process behind automated-decision making,

[159] Bayer (n 133), 2, 5.
[160] Llansó et al (n 143), 10-11.
[161] Gillespie (n 118), 19.
[162] Nicholas Diakopoulos, 'Algorithmic accountability: Journalistic investigation of computational power structures' [2015] Digital Journalism, 1, 4 <https://computingeverywhere.soc.northwestern.edu/wp-content/uploads/2017/07/Diakopoulos-Algorithmic-Accountability-Required.pdf> accessed 21 September 2022.
[163] Article 19, 'Submission of Evidence to the House of Lords Select Committee on Artificial Intelligence' [2017] 7 <https://www.article19.org/wp-content/uploads/2017/10/ARTICLE-19-Evidence-to-the-House-of-Lords-Select-Committee-AI.pdf> accessed 21 September 2022.
[164] Lilian Edwards and Michael Veale, 'Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for' [2017] Duke Law & Technology Review, 41-54 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855> accessed 21 September 2022.
[165] Edwards and Veale (n 164). 55-59.
[166] ibid, 60-61.
[167] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

thereby definitely enhancing transparency and accountability.[168] However, as in most cases content moderation decisions will not touch upon users' personal data to assess the content, this provision is inapplicable, and a similar obligation can only be imposed through the DSA. Finally, the current lack of (satisfactory) explanations is closely related to another problem when it comes to algorithmic content moderation decisions, which is lack of accountability.

3.2.3. Pointing a finger

Algorithms make mistakes. However, humans are standing right behind them. Now the question arises: Who is responsible for these mistakes? The question of accountability is one of the most important ones in general and when it comes to algorithmic decision making, the legislation provides no clear answer.[169] Firstly, algorithms do not yet have a legal personality and cannot be held responsible themselves. Secondly, since many algorithmic decisions cannot be fully understood or explained, it is impossible to point a finger at a single actor out of all human influences embedded into the algorithms.[170] Starting from the platforms that use the algorithms, people who get to define concepts such as 'hate speech', programmers that encode these definitions, content labellers 'training' the algorithms, to the users who (intentionally or not) violate the rules, there is a number of potential 'suspects' to look at. It is essential to keep this in mind when assessing accountability for an algorithmic decision. Thirdly, when it comes to unlawful speech, it seems unfair to hold the service providers accountable for something posted without their approval or oversight. Moreover, since general monitoring is strictly prohibited, service providers are even prevented from constantly monitoring the uploads.[171] And lastly, many posts today are made by anonymous users, fake profiles, or not even people but bots, and it was (and still is) almost impossible to hold the speaker accountable.[172] For these reasons, tendencies towards intermediary liability used to be strong and had to be contained in order to prevent forcible implementation of imprecise, overly-broad-filtering, and underdeveloped algorithms.[173] Although artificial intelligence has progressed significantly in the last couple of years, intermediary liability still remains peripheral in the newest legislative proposal. However, some of the implemented regulations still caused a similar effect, as it will be later explored in detail, and

[168] See, for example, Andrew D. Selbst and Julia Powles, 'Meaningful information and the right to explanation' [2017] International Data Privacy Law, Vol. 7, No. 4, 233, p.242 <https://doi.org/10.1093/idpl/ipx022> accessed 23 September 2022.
[169] Diakopoulos (n 162), 5.
[170] ibid.
[171] Article 15 of the 'Directive on electronic commerce' (n 135).
[172] Bayer (n 133), 7-8.
[173] Llansó et al (n 143), 12.

this does mean that in most cases there is still no answer on who is to blame. At least not a satisfactory one.

4. Where We Are Now

4.1. Current Regulation

Artificial intelligence and the platforms that use it are still regulated by the e-Commerce directive,[174] which was adopted over 20 years ago. This directive makes the foundational legal framework of online services in the EU.[175] However, much has changed since its adoption. Firstly, its definition of service providers, eligible for exemption from liability, states in Article 2 that these are 'any natural or legal persons providing an information society service'. Which is to say any service 'normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services'.[176] The problem encountered is that this definition must be interpreted broadly if non-editorial social media platforms that usually provide their services for free are to be included. Conversely, the provisions can be interpreted to only affect the platforms having no knowledge of what their users are sending, transmitting, or storing (e.g. email).[177] This was also confirmed in the case of L'Oréal v eBay,[178] when the European Court of Justice ('the ECJ') found that eBay was not entitled to rely on the exemption from liability provided by Article 14 of the Directive because it played an active role, assisting in the sales. Further examples of similar reasoning can be found in the judgements of the ECHR in cases Delfi v Estonia and Index v Hungary,[179] where it was decided that a news portal can be liable for third-party comments. Luckily, these rulings were followed by the Council of Europe's Recommendation proclaiming that 'States should ensure that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store'.[180] Hopefully, these recommendations have put an end to any contrary tendencies.

The second problem arises from the fact that the e-Commerce directive is still a directive, which

[174] 'Directive on electronic commerce' (n 135).
[175] The European Commission, e-Commerce Directive, Policies, 2021, <https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive> accessed 23 September 2022.
[176] Article 1(2) of the Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 217/18.
[177] ibid.
[178] Case C-324/09 L'Oréal and others v eBay [2011] ECLI:EU:C:2011:474.
[179] Delfi AS v Estonia (n 129); MTE and Index v Hungary, App no 22947/13 (ECtHR, 2 February 2016).
[180] Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries (adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies) at 1.3.7.

must be interpreted and implemented into national legislation of Member States. This leaves us with 27 different solutions to the same problem and imposes a lot of burden on the service providers to keep track of the differences. The Internet and the platforms governing it are a ubiquitous phenomenon and cannot be isolated to affect just one State, especially if the goal is achieving a fully functioning digital single market. Having said that, freedom of expression and its legal safeguards are still governed by State regulations such as the German Network Enforcement Act on the one hand, which imposes 'hard' obligations on the service providers with very strict removal timeframes and substantial sanctions.[181] A notorious example of how this can lead to over censorship is the removal of a satirical post in The Titanic Magazine, that was intended to ridicule the previously censored Alternative für Deutschland's (AFD) anti-muslim post.[182] On the other side of the spectrum, there is the group known as the Digital 9+, including countries such as Sweden, Poland, or the Netherlands, that take a 'light approach', implementing measures such as notice and action mechanisms accompanied by voluntary, prior-control measures of the platforms to 'swiftly' remove 'clearly illegal' content.[183] What can be considered 'clearly illegal' needs to be determined separately, but the requirement of 'swift' action definitely implies a more relaxed approach. The years of struggle between the actors involved and the two main legislative currents resulted in the new proposal for the Digital Services Act.[184] And although the proposal deals with many of the negative remarks to the German approach, its influence is undeniable as can be seen in the following Chapter.

4.2. Digital Services Act

The proposal for the new Digital Services Act was introduced in December 2020 and the regulation is meant to upgrade the existing rules and overcome the existing fragmentation to ultimately reign in Big Tech companies in Europe.[185] Firstly, the DSA includes a new and wider definition of 'online platforms', stating that these are 'providers of hosting services which, at the request of a recipient of the service, store and disseminate information to the public' (Article 2(h)) This definition clearly includes social media networks and similar platforms, while other types of providers are still regulated as 'intermediary services'. However, what is still not precisely

[181] Lea Duplan, 'France, Germany and Illegal Content Online: Where to, Europe?', June 30, 2020 <https://apcoworldwide.com/blog/> accessed 21 September 2022.
[182] Bayer (n 133), 14.
[183] Duplan (n 68).
[184] Proposal for the Digital Services Act (n 138).
[185] Clothilde Goujard and Samuel Stolton, 'Europe reins in Big Tech: What you need to know', November 25, 2021 <https://www.politico.eu/article/europe-digital-markets-act-dma-digital-services-act-dsa-regulation-platforms-google-amazon-facebook-apple-microsoft/> accessed 21 September 2022.

defined is the 'illegal content', where a circular definition states that it entails everything considered illegal in the EU and the Member States (Article 2(g)). To reflect on the problem of 'hate speech' and its mostly non-existing or inadequate legal definitions,[186] this means that online platforms still have to determine what they consider to be 'hate speech' and then remove all such content.

Furthermore, the DSA makes a difference between micro or small enterprises (Article 16), very large platforms (Article 25), and everything in between. All these categories are subject to different sets of obligations with the highest demands imposed on the very large platforms, with over 45 million average monthly users (Article 25(1)). This is fully in accordance with the fact that such platforms have the biggest impact on the freedom of expression as well as substantial financial resources at their disposal.[187] Their influence on society and the level of power concentration, even inspire ideas of inflicting public service obligations on these giants.[188] All things considered, it can be argued that the current approach draws inspiration from such ideas. For instance, if the current DSA proposal is adopted, the very large platforms will have to perform once-a-year systemic risk assessments of the impact of their operations on human rights and freedoms (Article 26). Then they will have to decide on and implement mitigation measures, such as content moderation and curation algorithms, to reduce the risks detected (Article 27). They will perform yearly audits at their own expense (Article 28), publish content moderation reports every 6 months (Article 13 and 33), and make available their recommendation system's parameters with an option to modify them (Article 29). Lastly, they will have to appoint one or more compliance officers to oversee compliance with the DSA (Article 32). They will, of course, have to comply with all other due diligence obligations listed in Sections 2 and 3 as well, such as notice and action mechanisms, reasoned explanations, expedient removal of reported content, and provide internal complaint-handling mechanisms. All these obligations are to be followed by substantial financial sanctions for failed compliance (Articles 58 and 59). Hence it is obvious that there are considerable demands on the platforms and even possible disputes emerging from internal complaint procedures are to be solved by special, out-of-court dispute settlement bodies (Article 18). This is why it can be claimed that online platforms, especially the very large ones, will increasingly resemble public institutions offering public services.

On the other hand, when it comes to State obligations, the biggest change is the mandatory designation of one or more competent authorities for monitoring compliance, one of which will

[186] Finck (n 126), 4.
[187] Llansó et al (n 143), 10-11.
[188] Bayer (n 133), 10.

be deemed Digital Services Coordinator and be responsible for the enforcement of the Regulation (Article 38). These Coordinators will have to cooperate among themselves, with other national competent authorities, the Board, and the Commission, allowing a degree of supervision at the national and EU level. However, there is much to be questioned. Although the Coordinators will be responsible for the enforcement of the Regulation, they have no specific obligations or duties. What they do have are powers to access the data of online platforms, request information, perform inspections, and receive explanations about suspected violations (Article 41). They would also presumably control the reports and audits of the platforms. However, what this means is that the Regulation allows but does not oblige inspection of the providers. It appears that it is left to the States, or to the Coordinators themselves, to determine what has to be done to assure compliance. Then the extent to which they can protect users' freedom of expression greatly depends on their qualification, time, and resources. To draw a parallel to the GDPR, one of its biggest critiques is lack of compliance due to insufficient financing and staff members, as well as stalling tactics deployed by the companies.[189] It is not unreasonable to assume that a similar scenario could happen with the DSA if nothing changes.

To conclude, it seems the only thing forcing platforms into compliance will be the way Coordinators exercise their powers. Namely, how often and how high they fine the companies. This again brings us back to the beginning of the discussion, because if the platforms are sanctioned too often and in substantial amounts, they will tend to over-block the content. Furthermore, such tendencies are also supported by the obligation of implementing mitigation measures. This will certainly lead the platforms with a high risk of unlawful content occurrence to implement algorithms preventing such content from even being published. All things considered, there are many reasons to conclude that forcibly turning Marc Zuckerberg into a public servant of the EU will not change the current 'block first think later' strategy which has managed to turn censorship into a global phenomenon. Nonetheless, in the following Chapter, a few suggestions will be made as to what possible ways forward lay ahead.

5. Ending the Age of the 'Filternet'[190]

Algorithms have become necessary protectors of our freedom of expression, but it appears that

[189] Adam Satariano, 'Europe's Privacy Law Hasn't Shown Its Teeth', Frustrating Advocates, NY Times, April 28, 2020 <https://www.nytimes.com/2020/04/27/> accessed 7 December 2021.

[190] Cory Doctorow, Europe's Digital Services Act: On a Collision Course With Human Rights, Electronic Frontier Foundation [2021]
<https://www.eff.org/deeplinks/2021/10/europes-digital-services-act-collision-course-human-rights-0> accessed 22 September 2022.

they are also its biggest threat. In this Chapter, a brief overview of the most prominent and important safeguards and measures for protecting the freedom of expression will be provided.

5.1. Multistakeholder Approach

As discussed, governance of free speech is no longer a 'two-way street'.[191] Today, people are censored, surveilled, and their freedom of expression is threatened not only by governments but also by various private actors operating across borders and jurisdictions.[192] The way to respond to this pluralist form of speech governance could be taking the multistakeholder approach.[193] This is especially important when determining the values to be protected and goals to be pursued. Therefore, the desired approach should be enabling experts, platform operators, governments, and the people to stand side by side, with dialogue as preferred means of designing the policies. Experts and governments are already cooperating, but this can be brought to a higher level. One way of enhancing this cooperation could be using crowdsourcing as a tool. Learning what the people think and taking it into consideration can be a powerful way of reaching a sense of partnership between the public and the governments.[194] This is also a reason why the 'the wisdom of the crowd' theory[195] is so appealing, but it must be observed *cum grano salis*. Perhaps general opinion towards a potential definition or a desired value could be extracted and taken as a parameter for the final decision. Or maybe the public could be offered more possible definitions to see which one it prefers. After all, if all invested parties participate in designing the policies and feel that their views are being considered, they will most certainly be quicker to accept and respect the policies made.[196]

5.2. Co-regulation

As it was mentioned in the previous Chapter, the most important decisions should not be left

[191] Balkin (n 114), 4.
[192] ibid.
[193] See, for example Natali Helberger, Jo Pierson and Thomas Poell, 'Governing online platforms: From contested to cooperative responsibility' [2018] The Information Society, Vol. 34 No.1, 7 <https://www.tandfonline.com/doi/pdf/> accessed 21 September 2022.
[194] OECD, Citizen participation in policy making, Government at a Glance [2017] OECD Publishing, Paris, 190 <https://www.oecd-ilibrary.org/docserver/gov_glance-2017-67-en.pdf?expires=1663938480&id=id&accname=guest&checksum=52352A42AD1CD62F662BBA5931002480> accessed 21 September 2022.
[195] For a deeper understanding of the theory, see James Surowiecki, *The Wisdom of Crowds* (New York: Anchor Books, 2005).
[196] For a brief analysis of the Canadian multistakeholder approach to internet governance and its success, see Mark Buell, 'Why multistakeholder policymaking works' [2019] Policy Options Politiques, <https://policyoptions.irpp.org/fr/magazines/> accessed 21 September 2022.

solely to the service providers. If co-regulatory bodies in journalism, public broadcasting, and advertising can exist, why are social media councils out of discussion? Co-regulatory bodies comprising of both government and private companies' members could be established[197] to draft Codes of Conduct or Codes against discrimination and hate speech and oversee their implementation. Questions as important as drafting and overseeing the implementation of key principles when handling unlawful speech should not be left completely in the hands of private entities since not only are they inclined to pursue their own interest, but this also leads to lack of democratically legitimated safeguards and enforcement regimes.[198] Moreover, Member States and the EU need to take some responsibilities and obligations onto themselves. For instance, the proposed DSA regulation imposes obligations of audits and risk assessments on the platforms. A question emerges, why is there no obligation of the State Authorities to conduct audits or risk assessments? These, together with stronger control powers of State bodies (or the newly established Digital Service Coordinators) are necessary to achieve effective governance.[199] Furthermore, the State Authorities should also have an obligation to conduct regular inspections. To emphasise this once more, State Authorities should not just have the power to conduct them but be obliged to do so. Like sanitary inspections of bars and restaurants or inspections of work conditions, so could 'fundamental rights' inspections be mandatorily conducted on a yearly basis. Lastly, instead of relying on private, out-of-court mechanisms, Member States' courts need to be strengthened with judicial review as preferred means of solving any possible disputes.[200] As Abraham Lincoln famously declared 'law without enforcement is just good advice' and the suggested amendments are just some basic steps that would concretise Member State and EU roles in protecting freedom of expression. These steps would undoubtedly pose an additional financial burden on the States, but they are certainly a way towards a more effective protection of free speech.

5.3. The Deadlines

When it comes to decisions with major influence over one of the most important fundamental

[197] Llansó et al (n 143), 23-24.
[198] Julia Haas, 'Freedom of the Media and Artificial Intelligence' [2020] Office of the OSCE Representative on Freedom of the Media Freedom of the Media, 4 <https://www.osce.org/files/f/documents/4/5/472488.pdf> accessed 21 September 2022.
[199] See, for example Mark McCarthy, 'Transparency Requirements for Digital Social Media Platforms Survey and Recommendations for Policy Makers and Industry' [2020] p.22, 26 <https://www.ivir.nl/publicaties/> accessed 21 September 2022.
[200] Daniel Holznagel, 'The Digital Services Act wants you to "sue" Facebook over content decisions in private de facto courts' [2021] 4-5 <https://d-nb.info/123639982X/34> accessed 21 September 2022.

human freedoms, the deadlines in which these decisions need to be made ought to be clearly determined. Ambiguous terms such as 'without undue delay', 'expeditiously', or 'in a timely manner', should be avoided as they often result in misunderstandings and misinterpretations.[201] Especially when these need to be obeyed by private bodies and companies. Conversely, if the provisions stay as they currently are, some guidelines as to what is considered 'expeditious' or constitutes 'undue delay' ought to be drafted. Furthermore, it might also be useful to distinguish the deadlines based on certain parameters, such as the algorithm's calculation of the probability of unlawfulness or at least have mandatory human oversight for certain cases recognised as borderline. For instance, an algorithm could estimate the probability that certain content is unlawful. If the probability is higher than 50% the content should be blocked right away. However, if the probability is estimated to be lower, the deadline could be prolonged to allow for human review. Other measurements and parameters could also be considered. For instance, if there are several complaints to a certain post then the post should also be removed sooner since it is more probable that it is unlawful. In any case, current regulation, as well as the wording of the new DSA proposal, lean the platforms toward expedient censoring, leaving behind potentially detrimental consequences.

5.4. User Control

Increasing user control could have beneficial effects for the freedom of expression, but also for the users' experiences of the environment they participate in.[202] The new DSA proposal proclaims that users should be able to access the parameters of the recommendation filters, but the possibility of shutting off these personalised filters altogether would be a real step forward. However, even if one can imagine a 'get me out of my filter bubble' button, this would hardly help in cases of algorithms falsely labelling content,[203] which pose the greatest risk for the freedom of expression.

Therefore, a possible way forward could be the implementation of notice-and-notice mechanisms[204] similar to those implemented by the Canadian Copyright Act.[205] Notifying the uploader of a complaint against his/her content would allow him/her to respond and possibly

[201] For a detailed overview of problems associated with ambiguity in legal regulation, see Sanford Schane, 'Ambiguity and Misunderstanding in the Law' [2002] Thomas Jefferson Law Review; San Diego Vol. 25, Iss. 1, 167 <https://idiom.ucsd.edu/~schane/law/ambiguity.pdf> accessed 21 September 2022.
[202] Llansó et al (n 143), 23.
[203] For more, see, Haas (n 198), 3.
[204] What is Notice and Notice?, University of Regina, <https://www.uregina.ca/copyright/resources/notice.html> accessed the 21 September 2022.
[205] Articles 41.25, 41.26 and 41.27(3) of the Copyright Act (R.S.C., 1985, c. C-42).

justify his/her action. Considering the delicacy of hate speech issues, the user reporting the content would probably want to stay anonymous, but it would still give people a chance to resolve the issue without anyone getting censored. Of course, this would be a somewhat risky approach since it greatly depends on the good faith of all parties involved. On the other hand, as GDPR has so clearly demonstrated, even strong, explicitly proclaimed data subject rights do not necessarily guarantee more control over the exercise of such rights or empower the users if other basic requirements (such as transparency) are not met.[206] Therefore, in the absence of any such user-empowering mechanisms, increased transparency and better complaint mechanisms are the way forward. And especially in that case, guidelines as to what can be considered a satisfactory explanation and what it means to resolve complaints 'in a timely manner' must be set. Explanations such as 'the content violates the community guidelines' without any reference to specific articles violated or taking 28 months to reinstate falsely censored content[207] cannot be tolerated. In any case, enhancing human agency and participation is necessary to make sure that the Internet is an open and friendly environment that nobody is discouraged from participating in.

6. Conclusion

Freedom of expression online is under great threat. The States have left some of the most important decisions, as well as their enforcement, to private, revenue-driven actors pursuing their own goals and interests.[208] However, not only have the States transferred some of their powers, but they have also implemented Draconian sanctions for persistent availability of unlawful content or failure to remove it in the moment it is spotted.[209] As thoroughly explored, the current scheme forces the companies to rely on unsophisticated and invisible algorithms. The mixture of these factors is a potential recipe for disaster.

The States need to take responsibility. They need to decide what is considered 'hate speech', 'discrimination' and 'fairness', what it means that 'content is clearly illegal', or to remove it 'in a timely manner'. The proposed regulation does not meet many of the requirements of legal texts. It is not clear or precise and it does not provide answers to certain key questions. Furthermore,

[206] Bart Custers and Aana-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' [2022] Computer Law & Security Review Vol. 46, 105727, p.16 <https://doi.org/10.1016/j.clsr.2022.105727> accessed 23 September 2022.
[207] Cory Doctorow, 'Instagram's slow-mo appeals court: A nanosecond to block, 28 months to review' [2020] <https://pluralistic.net/2020/05/17/cheap-truthers/#robot-sez-no> accessed 21 September 2022.
[208] Haas (n 198), 1.
[209] This conclusion was drawn in accordance with the analysis presented in Balkin (n 114), 30-33.

State bodies need to be given certain specific obligations and judicial review of platform decisions should be made more easily accessible. Discouraging people from seeking protection of their fundamental rights before State Courts cannot be accepted. It must be kept in mind that these complaints are not any 'regular' complaints. They deal with alleged violations of a fundamental human freedom and as such are too important to be pushed outside of the State's judicial system.

To conclude, all of us already live inside our little filter-bubbles, created by our perceptions and misconceptions, which makes communication and mutual understanding difficult. Including an additional layer of 'out-side' filtering on top of that only adds to the confusion. However, it appears this has become a necessity. The people have been given the stage to freely express themselves, and many are using it against the intended purposes of facilitating communication and enhancing understanding. This is why change is necessary. The States need to retrieve their powers and responsibilities, average users need to be heard, and platforms need only govern their communities after meeting the legal requirements. Human rights should be the basis on top of which to build, they need to be the floor rather than the ceiling.[210]

[210] Article 19 and Privacy International, 'Privacy and Freedom of Expression in the Age of Artificial Intelligence' (n 115).

TACKLING HATE SPEECH: A COMPARATIVE ANALYSIS OF THE REGULATION OF HATE SPEECH ON SOCIAL MEDIA IN GERMANY AND THE UNITED STATES

Morris Ameyaw[211*]

Abstract

This article provides a comparative legal analysis of how the German and US legal systems enforce rules regarding hate speech on social media. It dissects the laws regulating hate speech on social media platforms in these countries and the debates and considerations leading to their adoption. It also examines some ground-breaking judgments and what role these cases have played in shaping the current and upcoming laws on internet hate speech. The article also explores some of the challenges in the enforcement of these rules and other alternative solutions currently under consideration. The evaluation section of this article considers the regulation of hate speech on social media in both countries. It highlights some of the differences and similarities in these legal systems concerning this topic.

[211*] LLM Candidate and member of the Master's Honours Research Track, Maastricht University.

1. Introduction

In today's digital age, it is an undeniable fact that social media platforms are a gamechanger in the realm of communication. Nevertheless, their role in communication has not been entirely free of flaws. One of the problems that has been feverishly discussed and highlighted recently is their use for online harassment. This issue takes different shapes, and may include: cyberstalking, doxing, revenge porn, trolling, and catfishing.[212] The number of online harassment cases continues to soar at an alarming rate.[213] A survey conducted by Pew Research Center found that as of 2017, almost 41% of the American population had personally experienced online harassment in one way or the other.[214] What is more, 66% of the population had borne witness to online harassment inflicted on to another individual 'and 62% consider it a major problem'.[215] Most of these forms of online harassment include the presence of hate speech.

Though there is not a universal legal definition of hate speech, the United Nations has described the following in its Strategy and plan of action on hate speech:

> *'any kind of communication, in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor'.*[216]

People who engage in hate speech usually do this intending to hold some form of power over members of minority groups.[217] In the past, newspapers, cable television leaflets, and magazines served as mediums for the propagation of hate speech.[218] The development of social media platforms has provided hate groups a wider space to carry out their agenda.[219] This assertion is also supported by the fact that there is an endless list of social media platforms available to

---

[212] '7 Types of Online Harassment to Watch Out For [Infographic]' <https://www.digitalinformationworld.com/2019/03/infographic-how-to-handle-online-harassment.html> accessed 1 May 2021.

[213] Natalie Annette Pagano, 'The Indecency of the Communications Decency Act 230: Unjust Immunity for Monstrous Social Media Platforms Comments' (2018) 39 Pace Law Review 511, 535.

[214] 1615 L. St NW, Suite 800Washington and DC 20036USA202-419-4300 | Main202-857-8562 | Fax202-419-4372 | Media Inquiries, 'Online Harassment 2017' (*Pew Research Center: Internet, Science & Tech*, 11 July 2017) <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/> accessed 18 March 2021.

[215] ibid.

[216] 'UN Strategy and Plan of Action on Hate Speech 18 June SYNOPSIS.Pdf' 2 <https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf> accessed 11 May 2021.

[217] LJL Lederer and RD Delgado, The Price We Pay: The Case Against Racist Speech, Hate Propaganda, and Pornography (Hill & Wang Inc, US 1995) 131.

[218] Michael L Siegel, 'Hate Speech, Civil Rights, and the Internet: The Jurisdictional and Human Rights Nightmare Comment' (1998) 9 Albany Law Journal of Science & Technology 375, 381.

[219] ibid.

internet users today. Consequently, there is an urgent need for countries to regulate hate speech. Each state has its own legal tools for dealing with hate speech on social media because there is no overarching legal framework that can tackle it yet.[220] While some countries employ stringent measures to curb it, others appear to be more liberal in their approach.[221] Regulations put in place to control hate speech on social media platforms usually come into conflict with the freedom of speech, as guaranteed by the state's constitution, or other international conventions it has ratified.[222] An example is the United States. Based on the 'broad latitude' which social media platforms enjoy as per Section 230 of the Communications Decency Act of 1996 (hereinafter CDA), social media companies cannot be held liable for inappropriate content posted by their users on their platforms.[223] By contrast, Germany can force social media platforms to take down any 'manifestly illegal' post within twenty-four hours.[224] In Germany, the *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act) of 2017 (hereinafter NetzDG) regulates online harassment on the internet.[225] Social media platforms usually enforce these rules mainly by reacting to posts and profiles reported by users via content moderators - who then proceed to filter posts and remove the ones which infringe content rules - as well as by employing algorithms, which flag malicious posts.[226]

This article seeks to explain why the United States and Germany regulate hate speech on social media so differently. It will also investigate how the German and US legal systems enforce rules regarding hate speech on social media.

2. Hate Speech on Social Media in Germany

2.1. General Introduction

On October 1, 2017, the Network Enforcement Act, adopted by the Bundestag, entered into force.[227] With its primary aim being the improvement of law enforcement on social networks, the NetzDG is one of the leading legal documents from a western country to help fill the legal vacuum on matters of online hate speech.[228] One of the characteristics that sets apart the

[220] 'Hate Speech on Social Media: Global Comparisons | Council on Foreign Relations' <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons> accessed 1 May 2021.
[221] ibid.
[222] ibid.
[223] ibid.
[224] Network Enforcement Act (2017, amended 2021) s3(2)(2).
[225] 'NetzDG - Gesetz Zur Verbesserung Der Rechtsdurchsetzung in Sozialen Netzwerken' <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> accessed 1 May 2021.
[226] Celine Castets-Renard, 'Algorithmic Content Moderation on Social Media in EU Law: Illusion of Perfect Enforcement' (2020) 2020 University of Illinois Journal of Law, Technology & Policy 283, 291.
[227] Network Enforcement Act (2017, amended 2021) s3.
[228] Danya He, 'Governing Hate Content Online: How the Rechtsstaat Shaped the Policy Discourse on the NetzDG in Germany' (2020) 14 International Journal of Communication 23, 3746.

NetzDG from all other prior regulations on social networks in Germany, is that it imposes fines on social networks in case they are unable to fulfil their duty to remove reported 'manifestly unlawful' content within 24 hours.[229] Under the NetzDG, social networks are required to disclose the system they have set in place to prevent illegal content from circulating online.[230] Social networks are expected to create a suitable mechanism in fulfilment of the requirement for 'report and takedown procedure'.[231] Initially, the task force which was set up by the German Ministry of Justice to work closely with social networks such as Google, Facebook, and Twitter, focused their research solely on incitement to hatred and the use of symbols of unconstitutional organisations (Section 130 & 86a of the German Penal Code (StGB), respectively).[232] Their research culminated in the first draft of the NetzDG in April 2017.[233] However, the current version of the NetzDG covers an extensive list of offences that also includes treasonous forgery (§100a StGB), defamation of religions (§166 StGB), and public incitement to crimes (§111 StGB).[234]

2.2. Reporting Obligation

Section 2 of the NetzDG stipulates that social networks that gather over 100 complaints within a year must provide extensive reports, written in German, twice a year (mid-year and at the end of the year).[235] This report must indicate the concrete steps which have been taken by the social networks in dealing with the complaints on posted content that are not in conformity with the law.[236] In addition to this, Section 2(1) NetzDG contains a detailed list of all the other requirements that the report must contain. There are a myriad of reasons put forward by the legislator in justifying this reporting obligation. One of the ways in which these reports may be useful is to retroactively assess the efficacy of the NetzDG.[237] Furthermore, the obligation to provide these reports fosters transparency as it holds intermediaries such as Google Search accountable for the influential role which they play in terms of regulatory access of digital communication on social networks.[238]

2.3. Handling Complaints about Unlawful Content & Regulatory Fines

[229] Network Enforcement Act (2017, amended 2021) s 3(2)(2).
[230] ibid, s 2.
[231] ibid, s 3.
[232] Victor Claussen, 'Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the Context of European Legislation' 27, 117.
[233] ibid.
[234] Network Enforcement Act (2017, amended 2021) s 1(3).
[235] ibid, s 2.
[236] ibid.
[237] See page 20 of the first draft of NetzDG.
[238] Gespiegelt in der Diskussion um die rechtliche Zulässigkeit von Maßnahmen zur Suchmaschinenoptimierung („SEO"); s. *Lichtnecker/Plog* in *Paschke/Berlit/Meyer*, HambKomm Gesamtes Medienrecht, 3. Aufl. 2016, Abschn. 28: Werberecht der elektronischen Medien Rn 12.

Social network providers are obliged to set up a mechanism to 'maintain an effective and transparent procedure for handling complaints about unlawful content'.[239] Save for situations where social network providers have acquired permission from the judiciary that affords them more time to delete or block content that is 'manifestly unlawful', all social networks are supposed to take down or block any 'manifestly unlawful content' within the specified time. [240] The time limit with regards to 'unlawful content', however, is seven days and this time limit is equally subject to an extension where social networks have found that the facts surrounding the 'unlawful content' are circumstantial, or where a 'recognised self-regulation institution' has been tasked with deciding the unlawfulness of the content in question.[241] Per the NetzDG, a 'recognised self-regulation institution' is an institution that analyses content independently to ascertain their unlawfulness and is usually funded by various social network providers. There is therefore a distinction to be made between content that is just unlawful and content that is manifestly unlawful. The difference mainly lies in the fact that even though both forms of content are against the law, the categorization of content as 'manifestly unlawful' is more obvious–hence why they must be removed within twenty-four hours or less.[242] On the other hand, it is not a straightforward process to label content as 'unlawful' because it usually takes seven days for a 'recognised self-regulation institution' to complete its analysis of a potentially 'unlawful' content.[243]

It is considered a regulatory offence if the procedures laid out to deal with complaints regarding unlawful content or any of the reporting obligations stated in the NetzDG are 'intentionally or negligently' violated.[244] In other words, it does not matter whether a social network provider (e.g., Facebook) knowingly or unknowingly failed to comply with its reporting obligations. The onus lies with social media providers to put the necessary measures in place so as not to go against the NetzDG provisions. Such administrative offences shall be punishable by fines up to five million Euros.[245] It is however interesting to note that the 'effects doctrine' influenced the formulation used in Section 4(3). The effects doctrine is used to enable an enforcing state to still have jurisdiction in cases concerning offences committed by non-natives living in a foreign country so long as the conduct has an effect within the enforcing state.[246] It is commonly used as a system

[239] Network Enforcement Act (2017, amended 2021) s 3(1).
[240] ibid, s 3(2)(2).
[241] ibid, s 3(2)(3).
[242] ibid, s 3(2)(2).
[243] ibid, s 3(2)(3).
[244] ibid, s 4(1).
[245] ibid, s 4(2).
[246] Vaughan Lowe, 'International Law and the Effects Doctrine in the European Court of Justice' (1989) 48 The Cambridge Law Journal 9, 9.

of jurisdiction in antitrust law and competition law of the European Union.[247] Applied to the NetzDG, violations of this Act may still be subject to punishment regardless of the geographic location of the place the law was disobeyed.[248]

2.4. Shortcomings

Critics have dubbed the NetzDG a 'hastily drafted law'[249] which although 'well-meant',[250] is equally 'the opposite of good'[251]. A number of reasons has been listed in support of these hostile sentiments expressed in response to the NetzDG.

First, there is the fear that NetzDG will result in 'over-removal'. The notion of 'over-removal' concerns the fact that the enforcement of NetzDG may lead to content, which under normal circumstances must have been considered legal, being removed wrongfully.[252] This can be attributed to the pressure to escape fines and meet the necessary deadlines which could make social networks hastily remove content which they assume illegal instead of taking time to assess such content critically as would have been done by a language expert or in the court of law.[253] This, therefore 'turns private companies into overzealous censors to avoid steep fines, leaving users with no judicial oversight or right to appeal', as was expressed by the German Director at Human Rights Watch, Wenzel Michalski.[254]

Wenzel's statement links to another downside to the NetzDG–privatised enforcement. As has already been discussed, the assessment of which content is to be considered illegal is *prima facie* a duty of social networks. The problem with this, however, is that the judicial system is left out of this process, in that there is no need for a court order before content is removed.[255] What critics find even more disappointing is the fact that victims do not have any judicial remedies to help them autonomously request an appeal.[256] This puts the victims in a disadvantageous position due to the lack of a redress strategy.

Another aspect of NetzDG which is consistently under critique is the disconnect between free speech and democracy brought to light by this law. The Justice Minister at the time this law was

---

[247] ibid.
[248] Network Enforcement Act (2017, amended 2021) s 4(3).
[249] Claussen (n 232) 25.
[250] Nikolaus Guggenberger 'Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht' (2017) Zeitschrift für Recht Politik 100.
[251] 'Claussen - Fighting Hate Speech and Fake News. The Network En.Pdf' 25 <http://www.medialaws.eu/wp-content/uploads/2019/05/6.-Claussen.pdf> accessed 11 February 2021.
[252] H Tworek and P Leerssen, 'An Analysis of Germany's NetzDG Law' 3 <https://dare.uva.nl/search?identifier=3dc07e3e-a988-4f61-bb8c-388d903504a7> accessed 11 February 2021.
[253] ibid.
[254] 'Germany: Flawed Social Media Law' (Human Rights Watch, 14 February 2018) <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law> accessed 28 February 2021.
[255] Tworek and Leerssen (n 252) 3.
[256] ibid.

drafted, Heiko Maas, was very vocal about the importance of this law in fighting fake news and hate speech online.[257] In defending the NetzDG against critics who deemed the Act an intrusion on the freedom of expression in a democratic society, Maas who is also a member of the Social Democratic Party in Germany, stated that '[t]he freedom of expression also protects offensive and hateful statements. But it is not an excuse to commit crimes.'[258] Maas also considers the fight against online harassment not only to be the duty of the judicial system alone but also that of social media providers.[259] He believes that even though 'the freedom of expression encompasses critical, confrontational and obnoxious comments, it also has boundaries.'[260]

There is also the potential for anti-government demonstrations arising in light of deleted controversial content involving influential members of the government or this even leading to the Streisand effect.[261] The Streisand effect refers to the unanticipated result of content that was meant to be removed or hidden from the internet, being broadly publicised.[262]

2.5. Reforms

On June 18, 2020, a new law was passed to work hand in hand with the NetzDG which was still undergoing reform at the time.[263] This amendment was meant to further strengthen the fight against hate speech.[264] Its announcement, however, was met with heavy criticism.

The new reform seeks to broaden the application of the NetzDG to include video-sharing platforms, which stands to negatively affect small platforms or those that focus on a specific area of interest.[265] It not only calls for the instant deletion of unlawful content posted online but

---

[257] 'NetzDG: Heiko Maas Verteidigt Netzwerkdurchsetzungsgesetz Gegen Kritik - DER SPIEGEL' <https://www.spiegel.de/netzwelt/netzpolitik/netzdg-heiko-maas-verteidigt-netzwerkdurchsetzungsgesetz-gegen-kritik-a-1186118.html> accessed 28 February 2021.

[258] ibid.

[259] 'Medienpolitik: „Die Meinungsfreiheit hat auch Grenzen"' (*Medienpolitik.net*, 9 January 2017) <https://www.medienpolitik.net/2017/01/medienpolitik-die-meinungsfreiheit-hat-auch-grenzen/> accessed 28 February 2021.

[260] ibid.

[261] Tworek and Leerssen (n 252) 3.

[262] Sue Jansen and Brian Martin, 'The Streisand Effect and Censorship Backfire' (2015) 9 International Journal of Communication 656.

[263] 'Germany's Updated Hate Speech Law Requires Sites to Report Users to Police | Engadget' <https://www.engadget.com/germany-netzdg-update-171502170.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABzsQi9_NR-f-aOwrjMa5SX9-xiKYvAL5iaI3jIurNYyhyedy58aN7Emh07QGzlXI8reYmX1Pxy8WEV5_lZcDjQuBBxbAB4V_tOCCI9xa1660-KzunJZqsE9OWikCGGswy22Fzj8cGH4SS1iHKDkCpQtlytsmMh8x-kxZy_NtCPB&guccounter=2> accessed 4 March 2021.

[264] Philipp Grüll, 'German Online Hate Speech Reform Criticised for Allowing "backdoor" Data Collection' (*www.euractiv.com*, 19 June 2020) <https://www.euractiv.com/section/data-protection/news/german-online-hate-speech-reform-criticised-for-allowing-backdoor-data-collection/> accessed 4 March 2021.

[265] 'Eco on the German NetzDG Reform: "We Need a Transparent Approach to the Fight against Hate Crime on the Internet"' (*eco*) <https://international.eco.de/news/eco-on-the-german-netzdg-reform-we-need-a-transparent-approach-to-the-fight-against-hate-crime-on-the-internet/> accessed 4 March 2021.

additionally the new reform obliges social media platforms to transfer user data in the form of port numbers, IP addresses, and so on to the Federal Criminal Police Office (BKA).[266] The rationale behind this new measure is to ensure thorough prosecution of the people behind unlawful content and serve as a deterrent for individuals that engage in online hate speech.[267]

The problem with this approach is twofold: the onus still lies on social networks to decide on what qualifies as unlawful content and not on the judicial system, and once platforms transfer the data of their users, there is 'data collection through the back door', which, as Niema Movassat of The Left party describes it, will inevitably occur in practice.[268] This is because although the new reform allows users to protest against their content being deleted where the content in question complies with NetzDG standards, their data would have already been transferred to BKA by the time of their complaint.[269] This would already constitute a violation of their privacy, even if the data transfer was initially for a legitimate reason. Take for example the scenario where a Twitter user (Sally) posts a meme online, and his friend (John) replies with a harmless joke following which Sally responds with the comment 'Dude, I'm going to kill you!'.[270] Such a comment could be erroneously interpreted as a death threat and instantly deleted, and the user's data would be subsequently forwarded to BKA.

In an attempt to remedy this situation, the Green Party in the Bundestag proposed a measure known as 'Quick Freeze'.[271] The amendment, which was not passed, proposed a system where instead of transmitting a user's data to the BKA once social networks delete that particular user's content, only the deleted content would initially reach BKA and the user's data would be 'frozen' until the BKA requests it for further investigation.[272] According to Ann Cathrin Riedel, the chairwoman of 'LOAD – Association for Liberal Network Policy', an alternative solution is presently in the pipeline and it involves the creation of a database that will be used in targeting suspicious activities.[273]

There is also the issue of there not being any specific time limit for social networks to restore content that was incorrectly taken down under the pretext that it violated NetzDG standards. To this effect, Josphine Ballon, a member of HateAid, suggested that this shortcoming be addressed

---

[266] Anna Biselli, 'Netzwerkdurchsetzungsgesetz - Bundestag entscheidet über umstrittenes Gesetz gegen Hasskriminalität' (*netzpolitik.org*, 18 June 2020) <https://netzpolitik.org/2020/bundestag-entscheidet-ueber-umstrittenes-gesetz-gegen-hasskriminalitaet/> accessed 4 March 2021.
[267] Grüll (n 264).
[268] ibid.
[269] 'Germany's Updated Hate Speech Law Requires Sites to Report Users to Police | Engadget' (n 53).
[270] Grüll (n 264).
[271] Biselli (n 266).
[272] ibid.
[273] Grüll (n 264).

in the reform.[274] She also emphasised that to ensure the effectiveness of this task, it should not be the responsibility of overworked content moderators but rather an internal committee.[275]

Eco, the largest association of the internet in Europe, pleads for a broader interpretation of the condition regarding 'immediacy' and believes 'that companies should also be allowed to outsource or centralise the notification and redress procedure to a qualified body such as an external contractor.'[276] This will ensure the principle of fairness due to the neutrality of such external bodies.

The NetzDG has and continues to play a crucial role in hate speech regulation. Germany provides an example of the European perspective of online hate speech and how it is dealt with.

3. Hate Speech on Social Media in the United States

3.1. General

In the United States, the Communications Decency Act is currently the leading authority when it comes to regulating hate speech online. In 1995, when the then Senator, James Exon, initially presented the CDA, its primary aim was to combat 'obscenity and indecency online'.[277] According to Exon, 83.5 percent of pictures that were circulating on the internet before the adoption of the CDA were pornographic.[278] The debates surrounding criminalising the posting of salacious speech or pictures on online platforms–where children could easily access them–played a major role in the enactment of this law. [279] This is because the protection of minors from such content was and is at the heart of the CDA.[280] This view is also reflected by the *Reno* judgment.[281] However, in *Reno*, it was held that even though the CDA was meant to protect minors from being exposed to adult content, it violated the freedom of speech which adults were guaranteed under the first amendment.[282] This decision was based on the fact that the CDA had initially imposed a blanket restriction on adult content on the internet even though

[274] heise online, 'NetzDG-Reform: Gesetzgeber verstrickt sich in unauflösbare Widersprüche' (*heise online*) <https://www.heise.de/news/NetzDG-Reform-Gesetzgeber-verstrickt-sich-in-unaufloesbare-Widersprueche-4786964.html> accessed 4 March 2021.
[275] ibid.
[276] 'Eco on the German NetzDG Reform: 'We Need a Transparent Approach to the Fight against Hate Crime on the Internet'" (n 265).
[277] Pagano (n 213) 514.
[278] ibid.
[279] Sara L Zeigler, 'Communications Decency Act of 1996' <https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996> accessed 15 March 2021.
[280] William H Freivogel, 'Does the Communications Decency Act Foster Indecency' (2011) 16 Communication Law and Policy 17.
[281] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
[282] ibid.

adults had the right to consume such content. On June 8, 1996, the CDA entered into force.[283] Later, when social media platforms began to gain immense popularity and the cry for the regulation of free speech online became louder, the CDA was amended by representatives Ron Wyden and Chris Cox to address hate speech in the brand new Section 230.[284]

In his book, The Twenty-Six Words That Created the Internet, Jeff Kosseff dives deep into Section 230 of the CDA by 'explor[ing] the past, present, and future of the law'.[285] The title of this book is a reference to the impact of Section 230(c)(1) CDA: 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.'[286] For social network providers, this means that they can 'escape liability as a publisher' for content posted by their users which might be damaging or hurtful to someone else.[287] Therefore, even though the offended party might have a tortious claim against the user in question, they may not sue the social media company due to the Section 230 immunity it enjoys. The immunity social media platforms enjoy in the United States is unique in the sense that if a 'traditional media company' such as a newspaper outlet (print or digital) were to have published an article written by an individual to defame another, the newspaper could be held liable before the court of law.[288]

Section 230 CDA provides further protection to social network providers in Section 230(c)(2)(a) which states that

> *'any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected'.*

What this essentially means is that, if social media companies provide for a system of content moderation on their own volition to prevent 'obscene, lewd, filthy, […]' content from being made available to the public via their platforms, they will still enjoy immunity from liability even if the content in question is 'constitutionally protected'.[289]

---

[283] '47 U.S. Code § 230 - Protection for Private Blocking and Screening of Offensive Material' (*LII / Legal Information Institute*) <https://www.law.cornell.edu/uscode/text/47/230> accessed 15 March 2021.
[284] Pagano (n 213) 515.
[285] Kosseff Jeff, The Twenty-Six Words That Created the Internet (Cornell University Press 2019).
[286] Section 230 of the Communications Act of 1934 at 47 U.S.C (1996) s 230(c)(1).
[287] George Fishback, 'How the Wolf of Wall Street Shaped the Internet: A Review of Section 230 of the Communications Decency Act' (2019) 28 Texas Intellectual Property Law Journal 275, 277.
[288] 'Section 230: The Law at the Center of the Big Tech Debate | WSJ - YouTube' <https://www.youtube.com/watch?v=FHTc6s5YTbU> accessed 16 March 2021.
[289] Fishback (n 287) 285.

3.2. Cubby Case

In 1991, the Supreme Court held in *Cubby, Inc. v. CompuServe, Inc.* that an internet site is akin to a library.[290] This is because as mere distributors, internet sites could only be held liable for defamation only in cases, where they received complaints or notification of the offensive content and chose not to act.[291] This decision set the debate in motion with regards to why defamation laws that apply to traditional media must also apply to internet sites. This case was also paramount because cases that were later decided according to the Cubby ruling revealed the inadequacies of applying traditional defamation laws to internet sites, which, in turn, led to the adoption of legislation on online hate speech.[292] One of such cases was the *Stratton* case.

3.3. Stratton Case

Stratton was one of the driving forces that led to the creation of Section 230 CDA.[293] In this case, a user of an online computer service known as Prodigy anonymously posted on Prodigy's 'Money Talk' bulletin board that an investment company called Stratton Oakmont had indulged in fraudulent activities during an initial public offering.[294] As a result, Stratton Oakmont, Inc. started defamation proceedings against both the anonymous user and Prodigy.[295]

On May 24, 1995, the New York Supreme Court held that since Prodigy had voluntarily decided to moderate content under its content guidelines, the existence of 'board leaders' tasked with enforcing these guidelines and due to its 'use of a software screening program which automatically [pre-screens] all bulletin board postings for offensive language', Prodigy could be classified as a publisher; hence, Prodigy was held liable.[296] The distinction between Prodigy and CompuServe, as well as the different outcomes of these two cases, lies in the fact that there was a conscious effort to monitor content in Prodigy whereas in CompuServe this element was lacking, and as a result Prodigy was held liable for its actions.

3.4. Carafano Case

Later in 2003, the ninth circuit court of Appeals explained Section 230 more liberally.[297] This case involved the famous Star Trek actress, Christiane Carafano who usually goes by the stage name

---

[290] *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).
[291] ibid.
[292] *Stratton Oakmont, Inc. v. Prodigy Services Corp.*, 776 F. N.Y.Misc. LEXIS 229 (N.Y.Sup. 1995).
[293] Freivogel (n 280) 21.
[294] *Stratton Oakmont, Inc. v. Prodigy Services Corp.*, 776 F. N.Y.Misc. LEXIS 229 (N.Y.Sup. 1995).
[295] ibid.
[296] ibid.
[297] Patricia Spiccia, 'The Best Things in Life Are Not Free: Why Immunity under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given Note' (2013) 48 Valparaiso University Law Review 369, 389.

Chase Masterson.[298] An anonymous user of Matchmaker.com created a fake profile impersonating the actress with the profile name 'Chase529', her picture, private address, and an email address that could automatically respond to all emails sent to it.[299] Consequently, she received a flood of messages sexually harassing her and threatening her son's life.[300] She vacated her home with her son, and they lived in hotels to avert any catastrophe.[301] Her lawsuit against the dating platform was unsuccessful because the court reasoned that even though Matchmaker.com was involved in the editing and choice selection process, it was still protected by Section 230 CDA immunity since it was 'a third party [who] willingly provide[d] the essential published content' and therefore Matchmaker.com was not deemed an information content provider in this case and as such freed from liability.[302]

3.5. Shortcomings

Subsections (c)(1) and (c)(2) of Section 230 are together known as the 'Good Samaritan' provision. This stems from the fact that this provision, in affording social media companies the level of protection it provides, considers these online platforms as the 'Good Samaritans' who are 'altruistically' 'blocking and screening offensive material' from circulating on the internet.[303] Critics, however, might strongly disagree with this title and might even be kind enough to suggest a title more befitting of Section 230: 'The Malevolent Provision'. This is because although Section 230 greatly favours social media companies, the opposite is true for both users and even non-users of these platforms who become victims of hate speech.

Indeed, Section 230 was created to promote the growth of social network providers, but years have passed and while magnificent growth of social media companies has been recorded, 'so has [the rise of] objectionable content'.[304] It has been 25 years since the enactment of the CDA, and social network providers have still not been held accountable for egregious crimes such as child porn, revenge porn, and hate speech which were and are still being committed under the auspices of social media platforms.[305] It is clear that if these social media platforms had not hosted the unpleasant content created by their users, *ceteris paribus*, victims of these heinous crimes would have remained unharmed as there would be no offensive content in the first place.

---

[298] Facebook and others, 'Actress' Suit Against Dating Service Rejected' (*Los Angeles Times*, 14 August 2003) <https://www.latimes.com/archives/la-xpm-2003-aug-14-me-startrek14-story.html> accessed 8 May 2021.
[299] *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003) 1121.
[300] ibid.
[301] ibid.
[302] ibid, 1125.
[303] Section 230 of the Communications Act of 1934 at 47 U.S.C (1996) (Long Title: Protection For 'Good Samaritan' Blocking and Screening of Offensive Material).
[304] Fishback (n 287) 289.
[305] ibid.

If this is the case, then it remains unknown why social media platforms are shielded from any fraction of blame seeing as they play a major role in the 'organisation' of such crimes.[306]

There is also the argument to be made that the broad immunity enjoyed by social media companies under Section 230 has produced the opposite effect of what Section 230 was meant to do for the internet and its users. In practice, however, social media companies continue to grow incautious by the day in relation to derogatory content posted on their platform. The carelessness exhibited by social media platforms obstructs the balance between promotion and protection and undermines the intentions of the legislature in enacting Section 230 CDA.[307]

3.6. Reforms

In the past 25 years of its existence, several proposals for a reform of Section 230 CDA have been put forth. One such proposal includes a bill that was proposed by Senator Hawley in 2019.[308] The bill which he titled Ending Support for Internet Censorship Act (hereinafter ESICA) essentially focuses on regulating political speech.[309] ESICA primarily deals with 'companies with more than 30 million active monthly users in the U.S., more than 300 million active monthly users worldwide, or who have more than $500 million in global annual revenue'.[310] Large tech companies, as defined above, could lose their automatic immunity under this bill.[311] Likewise, large tech companies could only benefit from immunity after passing an audit by a third party, specifically the Federal Trade Commission (FTC). Unless FTC can ascertain, by a qualified majority, that there is no political bias to a large tech company's mode of content moderation and the algorithms used, the company cannot gain immunity.[312] All costs incurred during the audit shall be borne by the large tech company that applied to the FTC for immunity and such an application will have to be renewed every two years.[313] ESICA therefore '[p]reserves existing immunity for small and medium-sized companies' since it focuses on the tech giants who fail to uphold their end of the bargain.[314] The pact which these tech giants continue to break concerns the fact that 'tech companies get a sweetheart deal that no other industry enjoys: complete exemption from traditional publisher liability in exchange for

---

[306] ibid.
[307] Pagano (n 213) 532.
[308] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. §2 (2019).
[309] Fishback (n 287) 291.
[310] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. §2 (2019).
[311] ibid.
[312] ibid.
[313] ibid.
[314] 'Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech Companies' (*Senator Josh Hawley*) <https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies> accessed 20 March 2021.

providing a forum free of political censorship'.[315] One downside to this proposal, however, is the so-called 'name and shame' clause included in ESICA which allows large tech companies to keep their immunity intact in a case, where a company has breached the above agreement, and the cause of this breach is attributable to an employee.[316] In such a case, the company can escape liability by 'publicly disclosing in a conspicuous manner that an employee of the [network] provider acted in a politically biased manner with respect to moderating information content; and terminates or otherwise disciplines the employee'.[317] Other shortcomings of ESICA include the fact that it is only limited to political speech and not hate speech online in general, and it is difficult to reach a supermajority within the FTC committee.[318]

Furthermore, the concept of an 'objective bad faith exception' was advocated by Ryan J.P. Dyer in an attempt to remedy Section 230 CDA.[319] Under this concept, courts would be able to assess the conduct of social media platforms on a case-by-case basis to see whether they acted in bad faith.[320] The results of such an assessment will ultimately influence the court's decision regarding whether Section 230 should be narrowed in that case.[321] Bad faith could be deduced from 'affirmative actions to enhance the content's unlawfulness'.[322] This could for instance involve the availability of tools that foster illegal content, creating webpages that specifically feature illegal content, or specifically decreasing the risk involved in such content being discovered by law enforcement.[323] Though this measure would go a long way to reduce automatic immunity by social media companies, it is feared that inconsistencies in judgments from different jurisdictions on similar cases would lead to its ineffectiveness.[324] The Digital Millennium Copyright Act (DMCA) is a federal statute that has often been proposed as a source of inspiration for a more efficient online hate speech legislation. The DMCA is focused on regulating copyright matters resulting from the use of the internet and technology.[325] As a result, critics continue to advocate for a replacement statute that would revolve around the DMCA:

> *'a DMCA-[modelled] statute would impose liability on a website for knowingly hosting unlawful content, deriving a benefit attributable to the offending content, and refusing to remove the unlawful*

[315] ibid.
[316] Fishback (n 287) 291.
[317] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. §2 (2019).
[318] Fishback (n 287) 292.
[319] Ryan JP Dyer, 'The Communication Decency Act Gone Wild: A Case for Renewing the Presumption against Preemption Comment' (2013) 37 Seattle University Law Review 837.
[320] ibid.
[321] ibid.
[322] Dyer (n 319) 861.
[323] ibid.
[324] ibid.
[325] 'Digital Millennium Copyright Act' (*LII / Legal Information Institute*) <https://www.law.cornell.edu/wex/digital_millennium_copyright_act> accessed 22 September 2022.

content after receiving notice of its illegality'.[326]

4. Evaluation

It is evident that while Germany pushes for a strict prohibition of hate speech online, the lines are quite blurred when it comes to the United States and how hate speech online is handled there. To gain a proper understanding of the reasons as to why these two countries differ in terms of hate speech regulation online, it is imperative to take a few steps back and analyse how hate speech, in general, is understood as a concept in both countries. In the United States, the notion of a 'free marketplace of ideas' arose in the *Abrams v United States* judgment.[327] In Justice Oliver Wendell Holmes' dissenting opinion, he drew inspiration from John Stuart Mill's utilitarian philosophy in his justification of free speech. Justice Wendell concurred with Mill in his reasoning that the truth could only be established if speech is unrestrained.[328] Mill believed that even if the discourse individuals have in establishing the truth ends up harming some people, it is still justified because establishing the truth would lead to the greater good of the collective.[329] Moreover, free speech in the US is enshrined in the first amendment of the constitution which states that 'Congress shall make no law […] abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.'[330]

In Germany, freedom of expression is laid down in Article 5(1) of the German Basic Law: 'Everyone shall have the right freely to express and disseminate his opinion by speech, writing and pictures […]'. In general, everyone should be allowed to express themselves without any 'censorship'[331]; however, '[t]hese rights are limited by provisions of the general laws, the provisions of law for the protection of youth, and by the right to inviolability of personal honour'.[332] In any case, Article 1 of the German Basic Law contains the most sacred text of the entire constitution: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.' The first sentence of this article supersedes all other principles in the German constitution.[333] It is, therefore, safe to say that any form of expression that seeks to put any human's dignity in jeopardy is strongly prohibited, and therein lies the first difference between both countries' approaches towards freedom of expression. This is subsequently

[326] ibid.
[327] *Abraham v. United States*, 250 U.S. 616,630 (Holmes, J. dissenting) (1919).
[328] ibid.
[329] "'Hate Speech in Constitutional Jurisprudence: A Comparative Analysis" by Michel Rosenfeld' <https://larc.cardozo.yu.edu/faculty-articles/148/> accessed 4 May 2021.
[330] Constitution of the United States of America (1789, amended 1992) amendment 1.
[331] Basic Law of the Federal Republic of Germany (1949, amended 2019) art 5(1).
[332] Basic Law of the Federal Republic of Germany (1949, amended 2019) art 5(2).
[333] *Life Imprisonment Case*, BverfGE 45, 187 (1977).

mirrored in their regulation of hate speech online. This is not to say that the importance accorded to free speech in the United States as guaranteed by the first amendment is non-existent in Germany. In fact, in *Lüth*, the Federal Constitutional Court held that free speech formed the basis of any 'liberal-democratic constitutional order because it alone makes possible the constant intellectual debate and the contest of opinions that is its elixir of life'.[334]

Another point in which both countries differ is the impetus for the creation of the legal documents which regulate hate speech online. In the United States, the driving force for the creation of the CDA was the urgent need to protect the underaged population from explicit content on the internet.[335] Section 230 CDA was specifically put together following the developments that arose in *Stratton*. On the other hand, the driving force behind the NetzDG being passed was an increase in hate speech against minority groups, especially immigrants on the internet.[336] What becomes equally apparent here is the fact that in both countries, more vulnerable members of the social group were in danger of being exposed to some form of abuse and these laws were created to prevent that.

Another factor that sets both countries apart in terms of the rules put in place to deal with hate speech online is historical influence. In the same breath, the fact that history played a role in the development of both legislation can be considered a similarity. In Germany, due to 'the totalitarian dictatorship in the Third Reich', there is a strong responsibility to protect minority groups from hate speech.[337] For example, it is a criminal offence to deny the holocaust in Germany per §130 StGB. As a result, the *Rechtsstaat* (legal state) idea has been highly instrumental in shaping the rules laid down in the NetzDG.[338] *Rechtstaat* is a doctrine concerning a 'constitutionalised state' in which the law overly controls governmental power.[339] According to Danya He, *Rechtsstaat* comprises of five major facets, namely '(1) Existence, validity, and primacy of law (2) Supremacy of basic rights enshrined in the Basic Law (3) Validity of constitutional principles from the Basic Law (4) State organisation (5) Proper legislative procedure'.[340] These facets play a crucial role in Germany's decision to use a statutory regulation in the form of the NetzDG as opposed to entirely relying on 'self-regulation' by social media platforms in fighting online hate speech.[341] In the US, there still has not been a shift from the way hate speech is regulated online. To this day, the social media platforms self-regulate hate speech on their

[334] *Lüth Decision*, BverfGE 7, 199 (1958).
[335] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
[336] Jack Counihan, 'Ein Mogliches Modell Fur Die Reform Des Hassredegesetzes: Ein Vergleich Zwischen Irland Und Deutschland Uber Die Freie Meinungsausserung' (2020) 23 Trinity College Law Review 252, 252.
[337] He (n 228) 3749.
[338] ibid.
[339] Carl Schmitt, *The Crisis of Parliamentary Democracy* (6th edn, MIT Press 2000).
[340] He (n 228) 3750.
[341] ibid, 3748.

platforms, and they cannot be directly held responsible for the content they host on their platforms.[342] While Germany has moved from depending solely on self-regulation carried out by social media companies, the United States continues to hold on to its historically liberal 'marketplace of ideas' approach and in so doing provides social media platforms leeway in dealing with this issue.

In addition, there are specific criteria laid down in the NetzDG and Section 230 CDA indicating which social media platforms are affected by these laws. In general, all social networks which operate to earn profit are affected by NetzDG, according to Section 1 NetzDG. However, the bi-annual reporting obligations prescribed by NetzDG are only to be fulfilled by social networks that receive complaints above 100 during a calendar year and have above two million registered users.[343] Section 230 CDA, on the other hand, does not contain any delineation as to which internet platforms should be held accountable through providing annual reports. There is therefore a strong desire 'to promote the continued development of the internet and other interactive computer services and other interactive media'[344] at the expense of the dignity of individuals who may become subjects of ridicule on the internet. It defines an interactive computer service as 'any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server'[345]. While the definition of social networks in the NetzDG limits itself to only profit-generating platforms[346], it can be inferred from the CDA definition of interactive computer services that both profit-generating platforms and non-profit generating platforms are included in the definition[347].

One negative effect of managing hate speech on social media platforms which both countries seem to agree on is the chilling effect that it may cause. In his paper on this topic, Joshua Spector describes the US perspective of this concept as "an illusion of restraint and an unfixed barricade against the enforcement of Internet speech regulations that, save some purportedly effective and convenient software, would be unconstitutional."[348] In Germany, there is the assumption that social media platforms will be tempted to indiscriminately remove content so as not to incur any administrative fine.[349] The fear of going against the NetzDG will therefore lead to content being taken down even if such content is not illegal, and this will subsequently discourage users from

[342] ibid.
[343] Network Enforcement Act of Germany (2017, amended 2021) s 3.
[344] Section 230 of the Communications Act of 1934 at 47 U.S.C (1996) s 230(b)(1).
[345] ibid, s 230(d).
[346] Network Enforcement Act (2017, amended 2021) s 1.
[347] ibid, 177.
[348] Joshua Spector, 'Spreading Angst or Promoting Free Expression - Regulating Hate Speech on the Internet Conference: United States vs. European Union: Transatlantic Debate on Issues Close to Home: Hate Speech on the Internet' (2001) 10 University of Miami International & Comparative Law Review 155, 170.
[349] ibid.

freely enjoying their freedom of expression.[350] This could be very detrimental in a democratic society.

5. Conclusion

Hate speech continues to be a pervasive practice that affects the lives of all internet users globally. This article has revealed that the effectiveness of the two legal tools developed by the United States and Germany to combat online hate speech do not offer the same level of protective efficacy. The United States seeks to promote freedom of expression while still protecting individuals against hate speech on the internet. However, the immunity Section 230 CDA provides social media platforms seems to impede the government from constructively achieving the intended protection. Conversely, in Germany, there have been strict measures put in place to restrict social media platforms while moderating content. The hefty fines social media platforms stand to incur in the event of non-compliance with the NetzDG has not only enhanced hate speech regulation in Germany but has also been at the centre of criticism. In answering the question: "How do Germany and the United States differently regulate hate speech on social media?", it can be said that even though Section 230 CDA offers a more liberal approach with regards to social networks, as opposed to the austere approach of the NetzDG. Both legal tools are greatly influenced by their individual history in relation to free speech and the fear of the chilling effect that managing hate speech on social media platforms may cause. Despite these similarities, the NetzDG and Section 230 CDA differ in terms of scope, the driving force behind their adoption, and their general understanding of hate speech.

[350] ibid.

ITALIAN CONSTITUTIONAL COURT REJECTS THE GENERAL REFERENDUM ON CONSENSUAL HOMICIDE: A STEP BACK OR A NECESSARY SAFEGUARD OF THE VULNERABLE?

Linda Canuto[351*]

Abstract

This article deals with ruling no. 50 of 15th February 2022 of the Italian Constitutional Court. In fact, the Italian Constitutional Court has rejected the question for a general referendum aiming to partially repeal the Article of the Italian Criminal Code about consensual homicide. This decision is decisive as the referendum was an actual attempt to legalise forms of active euthanasia in Italy as Italian legislation does not allow active forms of euthanasia. In order to understand the implications of Ruling No. 50, this article will briefly illustrate Italian legislation on both active and passive euthanasia and the major legal cases that led to the proposal of this referendum. Furthermore, the ruling of the Court will be analysed so as to understand its grounds and determine the scope of this judiciary decision.

[351*] Linda completed her master's degree in law *summa cum laude* at University of Padua, Italy, with a dissertation on the children rights in online contracts and is now performing a traineeship at the local Civil Court. In addition to that, the Author worked as a tutor junior in her home university and has shown some interest in legal research through taking part in legal research groups and scientific publications. As fields of law are concerned, Linda is interested in civil law, comparative law and human rights.

1. Introduction

The Italian Constitutional Court has declared, through a press release issued on 15th February 2022, that the question for an abrogative referendum of Article 579 the Criminal Code has been declared inadmissible.[352] This decision was further explored in the subsequent ruling of the Constitutional Court, which will also be referred as 'the Court', dated 15th February, which was published in the official Gazette of the Italian Republic later on 2nd March 2022.[353] This article deals with the debate on consensual homicide, which occurs when the person asks somebody else for help to terminate their life. This specific constitutional question was raised as a tool to allow a form of direct euthanasia in Italy for severely ill persons who cannot independently take their life under the current legislation.[354] The ruling of the Constitutional Court does not only involve principles of law but deals with a highly discussed topic by the public and media. In fact, the general public responded with great interest in the referendum on this topic, while the ruling sparked widespread malcontent.[355] The Court blocked the question for the referendum deciding on technical lawful matters, and in doing so it refused to take a clear political position on active euthanasia and its limits. This paper will analyse the reasoning behind the content of the ruling of the Court in order to determine whether the Court's decision is consistent with the Italian Criminal Law system or is highly influenced by pressures from the political arena and the general public.

2. The Reasons of the Referendum, Previous Legal Cases and Discipline

The aforementioned decision of the Court concerns the constitutional legitimacy of the referendum on the homicide of a consenting person. A general committee presented to the Constitutional Court the question of setting a popular referendum to partially repeal Article 579 of the Criminal Code for the parts where it imposes a sanction on anybody who provokes the death of another person on specific demand of the victim or with their consent.[356] This question was made possible by Article 75 of Italian Constitution which states that: 'A general referendum

[352] Italian Constitutional Court, Press release 15th February 2022 <https://www.cortecostituzionale.it/documenti/comunicatistampa/CC_CS_20220215193553.pdf > accessed 23 February 2022.
[353] Italian Constitutional Court C-50/2022.
[354] Marcella Fortino, Prime note sulla pronuncia della corte costituzionale n. 50/2022, [2022], Nuova Giur. Civ., 449
[355] Nicoletta Cottone, 'Referendum eutanasia, depositate in Cassazione 1,2 milioni di firme' in Il sole 24 ore <https://www.ilsole24ore.com/art/referendum-eutanasia-depositate-cassazione-12-milioni-firme-AEOpdXo> accessed 23 February 2022.
[356] Referendum Eutanasia legale: liberi fino alla fine <https://referendum.eutanasialegale.it/il-quesito-referendario> accessed 23 February 2022.

may be held to repeal, in whole or in part, a law or a measure having the force of law, when so requested by five hundred thousand voters or five Regional Councils'.[357] This constitutional rule must be coordinated with Constitutional Law no. 1 approved on 1st March 1953, according to which it is the Constitutional Court that rules on the admissibility of the general referendum, while Articles 27 and 35 further stipulate the procedure of the question to the Court. To partially repeal Article 579 of the Criminal Code an organising committee was set up with the contribution of various organisations, associations and political parties in order to collect at least five hundred thousand signatures of voters with the purpose of demanding the Constitutional Court's permission to hold a referendum to repeal Article 579.[358] Over a million signatures were filed at the Court of Cassation for further control and approval; this procedure was fully completed on 15th December 2021 as the Court of Cassation considered legitimate the referendum and allowed its transmission to the Constitutional Court under the title 'Partial repeal of Article 579 of the Criminal Code (homicide of the consenting person)'.[359] In particular, it was asked to repeal Article 579 of the Criminal Code for the part that it provides for a custodial sentence for everyone who causes the death of another man with the consent of the latter. Also, the referendum demanded to repeal the second paragraph concerning the application of aggravating circumstances, particularly with regards to the dispositions of homicide in a given case.[360] As a result, Article 579 of the Criminal Code would only provide a custodial sentence for anyone that commits consensual homicide of a minor of age 18, a mentally ill person or a person who happens to be psychically debilitated as a result of any kind of illness or substance abuse, a person whose consent was extorted with violence, threat, suggestion, or deceit.[361]

What makes this case interesting is the reason behind the referendum question. In fact, we are not facing just another case of decriminalisation on popular request, but rather an attempt to recognise a form of active euthanasia in Italy and fill the legislative void on the matter. It is important to highlight that Italian law does not contain a rule permitting active euthanasia, which is also named consensual homicide, but only passive euthanasia, that is in other words assisted suicide. In an attempt to fill this legislative void, the Italian Parliament passed Law No. 219 of 2017 to cater to the need to provide suitable pain management and palliative care treatments and waivers of life-preservation treatments. Law No. 219 is a response to the ruling of the

[357] Marco Azzalini, La "scala Shepard" del fine vita. La consulta e l'imperativa road map dell'aiuto nel morire, tra tutela della vita e tutela del proprio sé, [2022], Nuova Giur. Civ., 421.
[358] Referendum Eutanasia legale (n 356).
Gabriella Lax 'Eutanasia legale depositato in Cassazione il quesito referendario' <https://www.studiocataldi.it/articoli/news/41691-eutanasia-legale-depositato-in-cassazione-il-quesito-referendario.asp> accessed 26 February 2022.
[359] Azzalini (n 357), 421.
[360] Fortino (n 354), 421.
[361] Referendum Eutanasia legale (n 356); Azzalini (n 357), 421.

Constitutional Court in the *Welby case* and *Englaro case* in which the Court dictated the constitutional value of the principle of a patient's informed consent to medical treatments suggested by a physician.[362] These two cases dealt with Italian citizens affected by an irreversible coma and highly debilitating incurable disease who demanded through their relatives, or personally when still possible, the right to a peaceful death.[363] In particular, the *Englaro* case dealt with a woman in irreversible coma for over 20 years, whose family started a legal battle in order to be authorised to terminate her sufferings by stopping the medical machines that kept her alive. On the contrary, in the *Cappato* case a man who was debilitated by an incurable and degenerative disease asked for help to terminate his own life as his illness prevented him from committing suicide.[364] An Italian journalist and activist, Marco Cappato, intervened in order to fulfil this man's wish abroad, where this was already permitted but had to face criminal charges as it would qualify as assisted suicide under Italian law.[365] In these occasions the Court confirmed the constitutional nature of the principle of informed consent as a full-scale right of the person grounded in the principles expressed in Articles 2, 13 and 32 of the Constitution and paved the way for the recognition of a right to self-determination in end-of-life choices.[366] Subsequently, the Italian Parliament intervened on this lawful matter with Law 2019 of 2017, whose title can roughly translated as 'Law on Informed Consent and Advance Treatment Arrangements'. In fact, Article 1 number 5 of Law No. 219 of 2017 grants everyone capable of acting 'the right to refuse or interrupt any healthcare treatment, even if necessary for their survival, also expressly including artificial provision of hydration and nutrition within this notion'.[367] It also establishes the procedure to follow in these circumstances for those who are minors or legally incapable. The informed consent, mentioned in the Law, must be acquired through the methods more consonant with the conditions of the patient and suitably documented through any convenient tool including a written text or video recordings. Regarding the physician involved, Article 1 at number 6 adds that the physician 'is bound to respect the express will of the patient to refuse healthcare treatments and to renounce to the same' and grants to the physician who complies to this law immunity to civil or criminal liability.[368] Law 219, actually, subordinated the approval to the end-of-life treatment to a number of conditions and to the correct completion of the procedure indicated by the law itself, in order to admit at the procedure only severely ill persons

[362] Welby v. Costitutional Court [2009] ruling no. 253 and Englaro v. Constitutional Court [2008] ruling no. 438
[363] Welby case (preliminary hearing judge of the Ordinary Court of Rome, no. 2049 of 23 July - 17 October 2007) and the Englaro case (Court of Cassation, First Civil Division, no. 21748 of 16 October 2007).
[364] Alessandra Leuzzi, La questione delle pratiche eutanasiche nell'ordinamento italiano, [2021], Diritto di Famiglia e delle Persone (Il), 1849.
[365] ibid.
[366] Welby v. Costitutional Court [2009] ruling no. 253 and Englaro v. Constitutional Court [2008] ruling no. 438.
[367] Law no. 219 of 2017, art 1.
[368] ibid.

and with the aim to make sure that the patient gives a consent free of any external influence. In addition to this, it operates in terms of the relationship of care and trust established between the patient and the physician. This law also coordinates with Law no. 38 of 15 March 2010 which guarantees the patient access to palliative care and pain management treatments. As a result of this legislation a patient who happens to be in the conditions requested by the law has the right to express by means of informed consent their will to refuse any treatment including lifesaving ones and ask for deep sedation while waiting to be assisted.[369]

Disciplining end-of-life choices is not just an Italian problem. As far as euthanasia is concerned, only few Countries have complete discipline. In fact, the law on the subject matter of the Netherlands provides for the non-punishment of a physician who satisfies requests for termination of life and requests for assisted suicide only if the professional conduct has been in compliance with the rules of due diligence and the guarantee procedures laid down by the law; Belgium and Luxembourg passed similar laws, respectively in 2002 and 2009, so that any physician who will cooperate in forms of euthanasia will not be charged with criminal sanctions if they follow the legal procedures and meet the requirements.[370] In Spain, the parliament passed the '*Ley organica de regulaciòn de la eutanasia'*, a general law on regulation of euthanasia, which regulates both passive euthanasia and assisted suicide. To apply this rule the patient must be affected by an irreversible and incurable disease that causes severe pain to request one of the two forms of euthanasia and they must then undergo the lawful procedure designed to grant that the consent to the procedure is free and aware. As a last step of the procedure a commission of physicians and jurists must approve the final procedure. On the other hand the situation is less clear in Portugal, as the law 109/XIV passed by the Parliament on this lawful matter is now subjected to a review of constitutional legitimacy.[371] From the point of view of case law, the Supreme Court of the United Kingdom allowed certain end-of-life proceedings, even when they concerned seriously ill minors; while the European Court of Human Rights has affirmed that euthanasia is not contrary to the European Convention on Human Rights, provided that the internal legal protocols are respected.[372]

---

[369] Luciano Salvatore Rocca 'Omicidio del consenziente, uno scenario scongiurato' in Altalex < https://www.altalex.com/documents/news/2022/02/23/omicidio-del-consenziente-uno-scenario-scongiurato> accessed 25 February 2022.

[370] Fabio Cembrani, L'eutanasia alla prova del referendum popolare abrogativo ed alle sue pericolose insidie - Italian petition to legalize euthanasia: controversial issues and perspectives, [2021], Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario), 963.

[371] ibid.

[372] Parfitt v United kingdom [2021], Lambert v France [2017], both explored in Edoardo Cipani, *Interruzione del trattamento vitale e miglior interesse del minore: il caso Parfitt v. Regno Unito,* [2021] Rivista Italiana di Diritto e Procedura Penale, 1145.

Back to Italian law on euthanasia, the referendum draws its legitimacy from the law which guarantees the right to refuse treatment but not the right to actively request to be subjected to euthanasia treatments in order to end one's life. In fact, patients suffering from debilitating and degenerative diseases do not have a tool, under Italian legislation, to request to put an end to their suffering before their natural death, as active euthanasia is not recognised and permitted by any law. Criminal law, in fact, not only punishes those who cause the death of another person, but also provides a sentence for anybody that helps a suicidal person to succeed in their intent to take their life, without directly designing any exception when the suicide is related to physically incurable diseases. This is expressed in Article 580 of the Italian Criminal Code. To fill this void, during the *Cappato case* the Court of Assizes of Milan, the local Court which was dealing with the trial, submitted a constitutional question to the Constitutional Court regarding the repeal of Article 580 of the Criminal Code on the grounds of incompatibility with Articles 2 and 13 of the Constitution. Article 2 of the Constitution expresses the subjective principle which puts the person at the centre of the legislation and Constitutional system, whereas Article 13 protects the freedom of speech and self-determination. Article 580 of the Criminal Code is also considered contrary to Article 117 of the Italian Constitution with regard to Articles 2 and 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), signed in Rome on 4th November 1950, ratified and implemented by Law No. 848 of 4th August 1955. In this case the Constitutional Court declared unconstitutional Article 580 of the Criminal Code, insofar as it did not exclude the punishment of those who, in the manner established by Articles 1 and 2 of Law No. 219 of 22nd December 2017, facilitate the fulfilment of the autonomously and freely formed intent to commit suicide'.[373] The Court specified that the person requesting the procedure must be indeed fully capable of making free and informed decisions and must be kept alive by life-support treatments; they must be also suffering from an incurable illness that causes a physical or psychological suffering that he or she considers intolerable.[374] This ruling is grounded in the circumstances that Article 580 of the Criminal Code is proved to be unconstitutional, as it violates Articles 2, 13 and 32 number 2 of the Italian Constitution as it does not allow a person who has the requirements requested by Law No. 219 of 2017 to be assisted by anybody in ending their sufferings.[375] According to ruling no. 242 of 2019, the Constitutional Court repealed the part of Article 580 which provides a punishment for anybody that facilitates the fulfilment of the autonomously formed will to commit suicide if the suicidal happens to be in the circumstances requested by Law No. 219 of 2017. After ruling no. 242 of

[373] Cappato v. Constitutional Court [2019] ruling no. 242.
[374] ibid.
[375] ibid.

the Court, a person suffering from an incurable illness that causes intolerable physical or mental pain has the right to commit suicide with the indirect help of a physician without the latter undergoing a criminal procedure. In particular, said physician cannot actively cause the death of the patients, as this hypothesis is regulated by Article 579 of the Criminal Code, but can facilitate their own suicide, for example by providing the most appropriate drug to pursue the intent of dying.[376] Of course, the Constitutional Court also disciplined a complex procedure that the patient must undergo in order to lawfully put an end to their life without criminal consequences for the physician who helps in making this possible. This procedure, in addition to surveying the informed consent of the patient, does include the indication of less definitive procedures, requires the approval of a specific committee identified in the regional ethic committee and guarantees the patient the right to change their mind until the very last minute.

Still after ruling no. 242 of 2019, suicide is only granted to patients who are able to commit suicide independently. The same opportunity is not offered to anybody who, despite being in the same circumstances requested by Law No. 219 of 2017, is not able to commit suicide autonomously as inflicting death upon another person is punished by Article 579 of the Criminal Code, even if this occurs with the consent of the victim. Lawfully, this goes under the definition of consensual homicide. Consensual homicide is, in fact, the rule whose partial repeal was questioned through the general referendum. As a matter of fact, the organising committee collected over one million two hundred signatures in order to question the Constitutional Court on the admissibility of a general referendum to repeal Article 579 for the parts that it punishes anybody who commits consensual homicide.[377] The aim of the committee, and thus of the general referendum, is to allow active euthanasia also for those who are not physically capable of committing suicide neither with an external help.[378] Here lies the big difference between Article 580, which was partially taken down, and Article 579: the former concerns anybody who facilitates suicide but does not directly cause the death of the patient, while the latter punishes those that directly cause the death of another person with the consent of the 'victim'. The difference itself may be subtle but is quite significant in the life of those affected by an illness causing substantial and irreversible suffering.

3. Ruling of the Constitutional Court

On 15th February 2022, with a press release, the Constitutional Court declared the general referendum inadmissible on the grounds that it does not provide adequate safeguard for

[376] Salvatore Rocca (n 369).
[377] Cottone (n 355).
[378] Referendum Eutanasia legale (n 356).

vulnerable subjects.[379] While waiting for the official publishing of the complete ruling, the President of the Court has further articulated the decision in a separate press conference held on 16 February 2022.[380] The final ruling was published on 2nd March 2022 and reproduced the same motivation anticipated by the President of the Court and further explained the controversial decision.[381] The Constitutional Court declared to be sensitive to the issue of life-ending treatments and euthanasia but does not consider it safe to proceed to legitimate consensual homicide in the terms presented by the request of the referendum and without an express legislative intervention on the subject matter.[382] In fact, in ruling no. 242 of 2019 the Court had already requested the parliament to intervene with a legislative text to regulate such hypothesis but in the meanwhile the Parliament failed to do so as any proposal in that sense failed to get through the parliamentary discussion or did not even manage to be presented to the chambers of Parliament. While renovating its invitation for the Parliament to legislate on the question, the Court ruled that the referendum in its current formulation does not comply with the legal duty to preserve human life and safeguard the most vulnerable as formulated in the Constitution.[383] In fact, the remaining part of Article 579 that would survive after the repeal only provided a custodial sentence for those who commit consensual homicide towards minors of age, mentally ill persons, physically incapable persons and when the consent is obtained with an act of violence or of deceit. Thus, phrased this way, the remaining part of Article 579 would not provide the adequate safeguard for those who do not comply with these circumstances but could nonetheless find themselves in a vulnerable position.[384] According to the Constitutional Court this specific hypothesis could possibly turn out to be a threat because the question does not take into consideration all these circumstances where the boundaries between assuring the right to decide how to deal with life-ending treatments and harming others on the grounds of a false consent are not clear. In addition to this, the remaining part of Article 579 would not contain any reference to life-threatening or incurable diseases so as a result anyone would be able to access the procedure if their consent is formed correctly, without any connection to medical euthanasia.[385] Also, the Article as resulting after the referendum would not provide some guarantees such as the right to take a step back from the procedure by any minute and the supervision and approval of a professional committee or organ, all these safeguards on the contrary are present in both

[379] Italian Constitutional Court, Press release (n 352).
[380] Italian Constitutional Court, Press conference 16 February 2022 < https://player.vimeo.com/video/678310064> and <https://www.cortecostituzionale.it/documenti/comunicatistampa/CC_CS_20220221122715.pdf> accessed 26 February 2022.
[381] Azzalini (n 357) 421; Fortino (n 354), 449.
[382] Italian Constitutional Court C-50/2022.
[383] Italian Constitutional Court, Press release (n 352).
[384] Italian Constitutional Court C-50/2022.
[385] Italian Constitutional court, ruling no. 50 of 2022, Azzalini (n 357), 421.

Law No. 219 of 2019 and ruling 242 of 2019 of the Constitutional Court itself that dealt with the subject. Moreover, the Article would not make any mention of a medical procedure, nor it would not grant that the procedure would be carried out by a physician in safe and painless conditions. The Court also declared that it would be unsafe to subject this referendum to the general public as the phrasing does not appear to be clear with its implications. Furthermore, during the press release, the President of the Court added that the whole mediatic case that has arisen on this matter has had a deceiving effect on the real subject matter of the referendum so to be fair the Article resulting from the modify should reflect the real aim of the referendum or the question of the referendum should be at least clear in its implications.[386] Once again, the Court urged the Parliament to adopt a legislation on consensual suicide and life-ending treatments to put a full stop to the debate.

4. Reactions to the Judgement

The general public responded bitterly as this was considered to be a step behind from the Court regarding the freedom to determine one's fate in case of incurable disease and, thus, it was taken more as a political ruling than a legal one.[387] The President of the Court also pronounced on this as he does not agree with these allegations and reminded previous rulings in which the Court supported the right to a peaceful death for ill persons.[388] Doctrine, on the other hand, is divided. In fact, part of it welcomed this ruling as doctrine agreed with the bad phrasing of the question of the referendum.[389] Also, jurists shared the fear of the Constitutional Court that altering Article 579 of the Criminal Code in such a way might have paved the way to allow consensual homicides in which the consent was not clearly formed and did not comply with the requests of the Law No. 219 of 2017 and the previous rulings of the Court such as ruling no. 242 of 2019.[390] Other authors, on the contrary, have stated their disagreement with the judgment as they consider this ruling as a political one, thus agreeing with the general public, and have stated that the remaining part of Article 579 of the Criminal Code would have been helpful to severely ill persons if the text was coordinated with Law No. 219 of 2017. In fact, according to their opinion, a coordinated application of Article 579 and Law No. 219 of 2017 would have created enough clarity to allow active euthanasia without major inconveniences.[391] They also think that such an

[386] Italian Constitutional Court, Press conference (n 380).
[387] Caterina Pasolini, 'Dacia Maraini sul no della Consulta all'eutanasia: "L'esistenza appartiene a ognuno di noi e il suicidio è un diritto' in Repubblica <https://www.repubblica.it/politica/2022/02/16/news/dacia_maraini_sul_no_della_consulta_alleutanasia_lesistenza_appartiene_a_ognuno_di_noi_e_il_suicidio_e_un_diritto-337918043> accessed 26 February 2022.
[388] Italian Constitutional Court, Press conference (n 380).
[389] Salvatore Rocca (n 369).
[390] Salvatore Rocca (n 369); Azzalini (n 357), 421.
[391] Fortino (n 354), 449.

interest in active euthanasia manifested by the Italian population should not be overlooked because of technical issues.[392]

5. Conclusion and Considerations on the Matter

It is also important to state that probably truth is to be found in the middle of the two opposing doctrinal orientations. Certainly, Article 579 of the Criminal Code, as resulting from the repeal, would not be able to regulate euthanasia on its own and some cases that fall in the 'grey zone' would have been hard to solve. In fact, the proposed modification would not have made a clear distinction between severely ill persons and anyone who wants to end their life for any reason other than incurable illness. So technically speaking the Constitutional Court is certainly making a point. The referendum would probably have had better chances to pass through if the organising committee involved the Constitutional Court during the formulating process and before collecting the required signatures as the law also permits, but this was not the case.[393] Actually, the phrasing of the referendum did not correspond to the well means of the general committee and the resulting version of Article 579 of the Criminal Code could easily be distorted in favour of less than noble interests. On the other hand, some correct legislation would have been possible through a tight coordination between Article 579 and Law No. 219 of 2017 and with the aid of a constitutional oriented interpretation given by the Court itself in the aforementioned 'grey zone' cases.

Truth to be told, the Court refused to take a political side. To support this statement, it is important to notice that some coordination problems would have arisen from the referendum, but these could have been overcome with the help of the Court, as suggested by part of doctrine. This would require a solid judicial orientation of the Court, orientation that probably the latter was not ready to take on. Also, in any case where the Court would have had to determine the limits of active euthanasia, the decision would have been more political than technical as Italian law does not regulate this aspect. Political decisions are to be taken by Parliaments though, not by Courts. Surely, through this technical solution the Court ignored all the people who signed to take the referendum in order to grant access to active euthanasia.

For this reason, it is extremely important that the Government passes through legislation on this specific question in order to finally provide an answer to all the severely ill people who are waiting for a lawful way to terminate their sufferings. In fact, the population has clearly expressed

[392] ibid.
[393] Italian Constitutional Court, Press conference (n 380).

its opinion on providing a source of legal euthanasia, despite the indirect way, and the Parliament has the duty of complying with it.

Only time will tell what Italian population will be allowed to do regarding life ending treatments in case of degenerative diseases which do not allow to commit suicide. In the meanwhile, it is clear that this will not happen by the means of the aforementioned general referendum.

THE LEGALITY OF TARGETED KILLINGS UNDER THE IHRL AND IHL LEGAL FRAMEWORK

Miriam Martinelli

Abstract

In recent years, many States have conducted targeted killings operations against State Officials and high-ranking members of armed groups. The aim of the present paper is to analyse the legality of these operations and to assess their compliance with jus ad bellum, human rights law and international humanitarian law. The paper will analyse the exercise of the right of self-defence by resorting to the use of force through targeted killing, taking into consideration the existence of a restrictive approach and a more permissible one. Moreover, the paper examines the applicable legal framework, in order to assess the lawfulness of these operations, considering all the three legal frameworks, applicable on the basis of the specific case.

1. Introduction

In our contemporary world, States are also increasingly involved in military operations with non-state actors, rather than with States, sometimes in counter-terrorism operations. The resort to drones leads to considerable change, as they allow States to reduce economic costs due to the use of force, it permits the deployment of force in dangerous areas and eliminates the risk for drone operators. In addition, drones are defined as highly precise weapons, and they are 'very limited in terms of collateral damage'.[394] Drones themselves as weapons are not considered illegal, what may be unlawful is their employment without complying with IHL rules, the lawfulness of a targeted killing operation must be assessed in accordance with the requirements of IHL and IHRL. The UN Special Rapporteur, Philip Alston, on extrajudicial, summary or arbitrary executions, has stated: 'It is true that IHL places limits on the weapons States may use, and weapons that are, for example, inherently indiscriminate (such as biological weapons) are prohibited. However, a missile fired from a drone is no different from any other commonly used weapons, including a gun fired by a soldier or a helicopter or gunship that fires missiles. The critical legal question is the same for each weapon: whether its specific use complies with IHL'.[395]

2. Self-defence

In order to determine the legality of the use of force through targeted killing operations in another State, jus ad bellum requires the consent of the territorial state to the military operations, as otherwise it could be an infringement of the State's sovereignty. The use of force in other States' territory is strictly prohibited under international law, however three exceptions allow it; with the authorization of the territorial States in accordance with Article 20 ARSIWA, the right to self-defence and finally, an authorization of the UN Security Council under Chapter VII Un Charter.[396] In the absence of consent, two provisions of the UN Charter shall be considered, Article 42 and Article 51.[397]

Article 42 provides an exception to the general prohibition on the use of force with the authorization of the UN Security Council, the latter under the UN Charter has the primary responsibility of maintaining international peace and security.[398]

---

[394] L. E. Panetta, Director of Central Intelligence Agency, 'Remarks at the Pacific Council on International Policy', 18 May 2009, available at: https://www.cia.gov/news-information/speeches-testimony/directorsremarks-at-pacific-council.html.

[395] Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston. Addendum-Study on targeted killings, 28 May 2010, para 79.

[396] Articles on the Responsibility of States for Internationally Wrongful Acts (with commentaries), Article 20 UN Charter; Article 51, Article 42.

[397] Articles 42, 51 UN Charter.

[398] Article 42 UN Charter.

Article 51 of the UN Charter allows and protects the 'inherent right of individual or collective self-defence if an armed attack occurs against a member of the United Nations'. The present article shall be carefully analysed, to determine the legality of the strikes, in particular to avoid any attempt to stretch extremely the scope of the right of self-defence beyond the boundary set out by Article 51. It imposes on States the legal obligation to immediately report to the Security Council the measures taken pursuant to their right of self-defence.[399]

In Customary International Law the Caroline case provides the traditional definition of the right of self-defence, which is constituted by the following elements; necessity, no choice of means, jus bellum proportionality.[400] The ICJ held in the Legality of the Threat or Use of Nuclear Weapons Advisory Opinion that a rule of customary international law provides that 'self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it.'[401]

There is a controversial debate over the right of self-defence, being it characterized by ambiguities, an element which gives rise to controversies, and ambiguities is the extent to which States relies on the right to self-defence, not only in response to armed attacks, but also in anticipatory self-defence or in pre-emptive measures against persistent threat or a future attack. There are three different views, and the legality of military operations depend on the endorsed view. The restrictive one, allows the use of force only after the occurrence of an armed attack, contrarily the more permissive view extensively adopted by State practice and scholarship includes the possibility of resorting to force against a real and imminent threat. Finally, there is a third view adopted by US policy since the Bush administration, with the US Global War, which allows pre-emptive self-defence, with no imminent threat.[402]

In order to determine the legality, it is essential to understand in which categories the attacks carried out fall, more specifically whether they intended to respond to an immediate threat or to an alleged attack in the future. From jus ad bellum provisions, it is possible to conclude that a right to prevent future attack or a right to self-defence for future alleged attack are not recognised, therefore resorting to the use of force in these scenarios is unlawful. The wording and formulation of Article 51 suggest that a State can only invoke the right of self-defence in response to an armed attack that has already occurred, without referring to anticipatory or pre-emptive defence.

The US Government has officially adopted the position that under jus ad bellum States may

[399] Article 51 UN Charter.
[400] R. Y. Jennings, The *Caroline* and *McLeod* cases, *American Journal of International Law*, January 1938.
[401] International Court of Justice, Legality of the Threat or Use of Nuclear Weapon, Advisory Opinion of 8 July 1996.
[402] US National Security Strategy 2002.

exercise their right of self-defence, not only as a response to armed attacks that have already occurred, but also in response to imminent attacks before their occurrence, as in the targeted killing of Soleimani.[403]

3. The Applicable Legal Framework: When is a Targeted Killing Considered Lawful?

Once determined that the targeted killing is lawful under jus ad bellum, the next step consists of assessing its legality within the applicable legal framework governing the use of force by State, more specifically under IHL and IHRL. The UN Special Rapporteur, Philip Alston, confirmed its applicability also in times of armed conflict, as well as the HR Committee in its General Comment No. 31 which underlines that the two regimes of law are complementary.[404]

The following standards of IHL apply irrespective of whether the armed conflict involved States (international armed conflict) or between a State and a non-state armed group (non-international armed conflict) including terrorists as Al-Qaeda.[405]

The legality of a targeted killing, under the principle of distinction, also depends on the targeted person, namely who, when and on what grounds can be targeted.

First of all, targeted killings are lawful when the target of the operation is either a 'combatant', a 'fighter'[406] or a civilian who 'directly participates in hostilities'.[407] It is essential that the targeted killing is militarily necessary and it employs an use of force that is proportionate, more specifically, the use of force must be proportionate in a way that the anticipated military advantage is considered in light of the expected harm to civilians in the proximity. Moreover, all feasible measures shall be adopted to prevent mistakes and minimize harm to civilians.

Outside the context of an armed conflict, the legality of a killing would be regulated by human rights law's provisions regulating the use of lethal force, under which a killing is lawful only if it is required to protect life and therefore proportionate and if there are no other means to achieve the results, rendering the use of force necessary.

---

[403] Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations, December 2016.

[404] Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston. Addendum Study on targeted killings, 28 May 2010, para 29.

8 United Nations Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 26 May 2004, UN Doc. HRI/GEN/Rev.9 (Vol. I), para 11.

[405] A/HRC/14/24/Add. 6.

[406] International Institute of Humanitarian Law, The Manual on the Law of Non-International Armed Conflict, March 2006.

[407] Geneva Conventions Common Article 3, AP I, art. 52(1) and (2); AP I, art. 50(1); International Humanitarian Law Research Initiative, HPCR Manual and Commentary on International Law Applicable to Air and Missile Warfare, Harvard University Program on Humanitarian Policy and Conflict Research, 15 May 2009, (HPCR Commentary), section C.12.(a)<http://www.ihlresearch.org/amw/manual> accessed 15 February 2022.

Taking into consideration the precise requirements of IHL, in international armed conflict combatants may be targeted at any time and place according to Article 48 API.[408] Another category is the one of civilians who 'directly participate in hostilities', however its clear definition is the subject of controversy regarding two issues; the kind of behaviour that constitutes 'direct participation', and whether the membership in an organised armed group could be used a determining element to consider the person as 'directly participating in hostilities'. In this regard it could be helpful to examine the Interpretative Guidance on DPH issued by ICRC in 2009, according to which to be considered a DPH three cumulative requirements must be satisfied:

1. There must be a 'threshold of harm' that is objectively likely to result from the act or from a coordinated military operation of which that act constitutes an integral part;
2. The act must be the cause of the expected harm directly;
3. A belligerent nexus with the act must be present.[409]

If there is uncertainty regarding the civilian conduct which qualifies as 'direct participation in hostilities', it must be presumed that it does not classify as it.[410] Moreover, States imperilled by an armed attack led by NSA from the territory of another State can use force as self-defence in the territory of the State, if it is unwilling or unable to eradicate the threat posed by NSA. This was clarified particularly in the aftermath of 9/11 by UN Security Council's Resolutions 1368 and 1373, and by NATO who strongly condemned Al-Qaeda attacks.[411] Israel and the US have confirmed the existence of an armed conflict against terrorists, namely NSA.[412]

The principle of military necessity requires that the kind and degree of force employed shall contribute effectively to the achievement of a concrete and direct military advantage, showing the absolute necessity of that action as no other reasonable options exist that would permit to achieve the desired military advantage. The principle of necessity has a central role in IHL, as a long-established principles , moreover the ICJ held that the latter with both the principle of distinction and the 'Martens Clause' constitute one of the 'cardinal principles' of IHL, remarking the absolute importance of not causing unnecessary suffering to combatants.[413]

Another decisive element is the principle of proportionality in attack, a fundamental part of treaty and customary IHL, applicable in international and non-international armed conflict. The

[408] HPCR Commentary section A.1.(y)(1). The term 'combatant' is not defined in IHL, but may be extrapolated from Geneva Convention III, art. 4(A); Ryan Goodman, The Detention of Civilians in Armed Conflict, 103 Am. J. Int'l L. 48 (2009).
[409] Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, International Committee of the Red Cross, N. Melzer, 2009.
[410] Article 50 First Additional Protocol.
[411] United Nations Security Council, Resolution 1368 (2001), 12 Sept. 2001, U.N. Doc. S/RES/1368(2001); United Nations Security Council, Resolution 1373 (2001), 28 Sept. 2001, U.N. Doc. S/RES/1373(2001).
[412] A/HRC/14/24 Add.6.
[413] 1 International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, paras.78-79.

principle is codified in Article 51(4b) of the First Protocol Additional which provides that 'an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated' is to be considered as indiscriminate.[414] The proportionality character of the attack must be determined ex ante, in good faith, and very importantly on a case-by-case basis. A contributing element to assess the proportionality is represented by the 'military value' of the targeted person, which is determined by considering many factors such as the operational functions, rank, tactical position. This element was particularly discussed in the US targeted killing of General Soleimani, due to his high rank it was difficult to believe in the necessity of the attack, as he was not responsible for operational functions or tactics. Finally, the principle of precaution in attack set out several separate obligations to safeguard the civilians' lives.[415]

4. Legal Framework: International Human Rights Law

The lawfulness of a targeted killing shall be assessed also under the International Human Rights legal regime. The 'right to life' is protected by all the most relevant international conventions, including the International Covenant on Civil and Political Rights (ICCPR), the American Convention on Human Rights and the African Charter of Human and People's Rights. The European Convention for the Protection on Human Rights and Fundamental Freedoms provides in Article 2 that no one shall be deprived of his life intentionally, it also provides a closed list containing the permissible grounds for justifying the deprivation of an individual's life. International human rights law set out that the deprivation of life must not be arbitrary. The use of force shall satisfy the proportionality test and the requirement of non-arbitrariness, meaning the resort to the use of lethal force must be absolutely necessary to defend 'any person from unlawful violence.' The test of proportionality that must be considered in the human rights field is different from the one in IHL. In the McCann v UK case, the ECHR defined the limits of the test of proportionality to determine whether the use of lethal force was absolutely necessary, it concluded that the force employed 'must be strictly proportionate to the achievement of the aims set outs in sub-paragraphs of Article 2.'[416] The Court in assessing the legality of the deprivations of life subjected it to a careful scrutiny and analysis, in particular, in those instances in which

[414] First Protocol Additional, art 51(4).
[415] ibid, art 57(1); J.-M. Henckaerts & L. Doswald-Beck, Customary International Humanitarian Law. Volume I, Rule 15.
[416] McCann and others v. The United Kingdom, Application No. 18984/91, Judgment, 27 Sept. 1995 ; European Court of Human Rights, Guide on Article 2 of the European Convention, 30 April 2021 updated, <https://www.echr.coe.int/Documents/Guide_Art_2_ENG.pdf> accessed 1 March 2022.

lethal force is employed, 'taking into consideration not only the cautions of the agents of the State who actually administer the force but also the surrounding circumstances including such matters as the planning and the control of the actions under examination.'[417]

Considering targeted killing within the IHRL legal framework, two scenarios shall be distinguished; the first in which the operation occurs within the territory of a State, such as a law enforcement measure, and the second situation in which the killing is conducted outside the State's territory, for example for counter-terrorism measures. For the purpose of this thesis, I will focus on the second situation, as the Soleimani strike occurred outside the territory of the US.

In order to establish whether the use of lethal force satisfy the requirements of the absolute necessity tests, two questions shall be examined; first whether the use of force was absolutely necessary or there were other measures that could be taken alternatively, second, if there were no other means available, was the resort to the use of lethal force, instead of lower degree of force, absolutely necessary. According to this legal regime, other less harmful options shall be first considered, only after having determined that they are inadequate through a careful assessment it is possible to resort to force.[418]

The use of force shall always be necessary and proportionate, furthermore it shall be used only when it is necessary to protect against an imminent threat to life, trying to resort to alternatives before deciding to use force, such as arrest. The intentional killing of a person would be considered lawful only in the exceptional circumstance in which it is the only means to protect against an imminent threat to life, in particular law enforcement agents 'may shoot to kill only when it is clear that an individual is about to kill someone (making lethal force proportionate) and there is no other available means of detaining the suspect (making lethal force necessary).'[419]

In order to resort to the use of force through armed drones, it would be necessary to prove that the targeted person represents an imminent threat to others rendering the use of lethal force necessary.

The right to life is not an absolute right, meaning that exemptions and derogations are possible. Among the derogations from the prohibition of the deprivation of life, there is the death penalty, conditional on the requirement of Article 6 and actions carried out by law enforcement officials such as lawful arrest. Article 6 ICCPR provides that every human being enjoys the right to life, and prohibits the arbitrariness of the deprivation of life.

It is worth noting that a State providing consent to the activities of other States in its territory, has to comply with the obligations arising from the human rights instruments it has ratified. In

[417] McCann and others v. The United Kingdom, Application No. 18984/91, Judgment, 27 Sept. 1995, para 150.
[418] UN General Assembly, Art 3 of Code of Conduct for Law Enforcement Officials (General Assembly Resolution 34/169, annex, of 17 December 1979).
[419] De Shutter O., International Human Rights Law, Cambridge 2019.

particular, the State providing the consent to the activities of a State on its territory must comply with the human rights treaties ratified, by avoiding any violations of its own nationals' rights and by guaranteeing the respect of human rights within its jurisdiction, furthermore it has the obligation to ensure protection from violations of the right to life, including by the host State, to the extent it can do so.[420] During an armed conflict, the IHRL regime shall apply together with IHL.[421] The right to life is recognised by many international human rights instruments, and has acquired the status of customary norm, therefore States have the legal obligation to ensure its realization when resorting to the use of force, including extraterritorially.

The UN Special Rapporteur concluded that 'any positive action by a State , on its own territory or that of another State, must be carried out in compliance with its human rights obligations under all applicable rules of international law.'

5. Can States be Held Accountable for Extraterritorial Violations of Human Rights?

Most of the time the use of armed drones for targeted killing is carried out in the territory of another State, in a cross-border setting. The lethal use of force against persons outside the confine of the State, automatically entails a question on the accountability and responsibility of the State under the human rights treaties, to which it is a contracting party, for the actions performed extraterritorially.

Concerning the territorial jurisdiction of a State, it extends also beyond its borders through the exercise of effective control over the territory of another State as a result of an armed conflict or after obtaining the consent from the State. The exercise of effective control over the territory of another state, including the use of force over its territory, implies that the States has jurisdiction over the affected persons, and the State owes to them the protection of their human rights. Turning to the case in which the State do not exercise territorial control, it still has to comply with human rights law in relation to the actions of its state officials or agents, as 'jurisdiction' is not limited to a territorial definition, but also to the relationship between the State and the person over which it exercises its authority, power and control.[422] In General Comment No. 31, the HRC affirmed that States have to respect and guarantee the rights enshrined in the Covenant to 'all persons who may be within their territory and to all persons subject to their jurisdiction.'[423]

[420] ILC, 'Articles on Responsibility of States for Wrongful Acts' (2001) UNYBILC vol II, Pt Two, art 23.
[421] United Nations Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Agnes Callamard, 29 June 2020 ,UN Doc. A/HRC/44/38.
[422] ECtHR, Al-Skeini Case, § 136; UNHRC, Burgos Case, § 12.2.; IACiHR, Alejandre Case, § 23; IACiHR, Coard Case, § 37; Melzer N., Directorate- General for External Policies of the Union(Directorate B, Policy Department), Human Rights Implications of the usage of drones and unmanned robots in warfare, May 2013.
[423] General Comment No. 31, CCPR/C/21/Rev.1/Add.13, para 10.

Furthermore, in the case Sergio Euben Lopez Burgos v Uruguay the HRC held that this does not automatically lead to the conclusion that the State cannot be held accountable for acts of its agents carried out in another State, which violates Covenant's rights, in accordance with Article 5.[424]

It has been confirmed by the jurisprudence and advisory opinions of the most important international courts that States have to respect the Treaty obligations, of which they are contracting States, also outside their territory.[425]

The recent case of Georgia v Russia before the ECHR, has the Court had to determine whether Russia had jurisdiction over the location in which the violations occurred and if it had jurisdiction, whether it breached the obligations arising from the Convention. Georgia brought a proceeding against Russia, considering it responsible for the violation of human rights, in particular Article 2, 3, 5, 8 of ECHR during wartime in Ossetia and Abkhazia. The Court issued a ground-breaking judgement by considering separately the phase of hostilities and the following events, concluding that Russia had no jurisdiction over the territory during the active phase of hostilities, as due to the unstable situation caused by the war it is impossible to establish the existence of effective control and so absolving it from the respect of some human rights obligations. In particular, the Court considered that during 'military operations - including, for example, armed attacks, bombing or shelling - carried out during an international armed conflict one cannot generally speak of "effective control"over an area.'[426] Turning to the jurisdiction arising from State agent authority and control over individuals, the Court endorsed a different view from the past cases on the basis of the different scale of hostilities, linking the scale of the hostilities to the ability of exercising extraterritorial jurisdiction. In the present case it considered 'the large number of alleged victims and contested incidents, the magnitude of the evidence produced, the difficulty in establishing the relevant circumstances' to reach the conclusion that Russia did not exercise extraterritorial control, and it only confirmed Russia's duty to investigate the deaths arose during the conflict and that Russian authorities had 'effective control' over South Ossetia, Abkhazia and buffer zone only after the phase of hostilities. This recent case could lead to serious consequences as it creates 'a legal vacuum' during war conflict, furthermore it could weaken the protection guaranteed by the Convention and, at the same time, weaken its essential role of protecting human rights by refraining from judging over the active phase of hostilities. The Court did not succeed in establishing who had jurisdiction over people residing in

[424] HRC, Sergio Euben Lopez Burgos v Uruguay, No. 52/79, para 176.
[425] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, para 109.
General comment No. 31 (2004), *Coard and others v. United States*, 1999, para 37, *Al-Skeini and others v. the United Kingdom*, application No. 55721/07.
[426] Georgia v. Russia (II) [GC], Merits, App. No. 38263/08 (Eur. Ct. Hum. Rts. Jan. 21, 2021) para 126.

the territories involved, and adopted a different approach from case law and practice.[427]

The extraterritorially validity of human rights treaties obligations, meaning they apply to the conduct of a State also beyond the borders of its territory, has been affirmed also by the Inter-American Commission on Human Rights, the ICJ, and UN Human Rights Committee.[428] The use of armed drones have led to new challenges concerning the exercise of jurisdiction, as the State who employs the drones can execute the operation without having effective control over the territory or without having the targeted person in custody. However, the targeted killings of individuals through the employment of armed drones outside the territory of the operating State, implies that the targeted person is under the State's jurisdiction. In particular, the targeting of a specifically selected individual extraterritorially implies the exercise of ultimate control over the individual by the State, leading to the consequence that the State must respect the human rights treaty obligations.[429]

It would undermine the real purpose of human rights law to allow the following interpretation of the validity of human rights treaties according to which a State can perform violations of human rights provisions on the territory of another State, for which it would be considered liable if perpetrated on its own territory.[430] In conclusion, any action by a State, irrespective of whether it is its own territory or that of another State, should comply with human rights obligations arising from treaties it has ratified as well as customary law.

6. Conclusion

It is possible to conclude that the lawfulness of a targeted killing operation, as every military operation in IHL, shall be assessed on a case-by-case basis, through a careful analysis of compliance with jus ad bellum and IHL norms. The 9/11 aftermath has consented to powerful States to soften the traditional international law norms, searching, and building a sort of right to targeted killing.

If the restrictive theory of self-defence applies it almost certainly leads to the conclusion that targeted killings against preventive attacks, such as the Soleimani killing by the US, are unlawful. Once such strikes are defined as unlawful, it is essential to examine the consequences for the State that breaches jus ad bellum, however in the reality the State in question will likely escape

[427] K. Dzehtsiarou, Georgia v. Russia (II), 115 The American Journal of International Law, 282 (2021).
[428] Human Rights Committee, General Comment 31, CCPR/C/21/Rev.1/Add.13 (2004), para 10., Coard et al. v United States, Case 10.951, Rep No 109/99, IACHR, 29 September 1999, para 37.
[429] Droege, 'Elective Affinities? Human Rights and Humanitarian Law' (2008) 90 IRRC 501, N Melzer, Targeted Killing in International Law (OUP 2009) 51–2.
[430] Ocalan v Turkey, App No 46221/99, Judgment, 12 March 2003, para 93; Issa and others v Turkey, App No 31821/96, Judgment, 16 November 2004, para 71.

State Responsibility for its breaches as most of the time the States who carried out these operations are powerful state as well as Security Council's permanent member, such as the US, which would be able to veto on Security Council's Resolution, leading to impunity.

The problem in determining the legality and lawfulness of the targeted killings lies in the fact that there is no precise formula or test to properly weight the proportionality and the necessity of the attack. In my view, the use of these highly-precise weapons is not unlawful, but the assessment of the legality of the targeted killings operations has to be done considering all circumstances leading to their occurrence and verifying their compliance with every IHL's requirements. For these reasons, it is impossible to achieve a clear-cut outcome, but rather each targeted killing requires a proper assessment test.

RULE OF LAW IN TIMES OF CRISIS

An-Nikol Voynska[431*]

Abstract

The purpose of this article is to address the threats to the rule of law and provide suggestions for strengthening it. Particularly, the Coronavirus has challenged the implementation of this fundamental legal principle multiple times recently. The research notes the important role of the cooperation between States and its citizens in tackling this health crisis by applying the rule of law.

[431*] Second-year law student at the University of National and World Economy in Sofia, Bulgaria.

1. Introduction

The notorious health pandemic COVID-19 spread in 2019 worldwide and brought substantial changes in all spheres of social life. Inevitably, international and national law were affected as well, because of the States' actions in cases of emergency. In particular, the survival of core principles such as the rule of law and respect for human rights were challenged. The health crisis only highlighted the exceptional need to further solidify the fundamental principle of the rule of law. On the one hand, this principle is a milestone in any democratic society, but on the other hand in times of crisis it is exposed to risks of abuse of power by States. For this reason, we should be more self-aware and proactive in identifying ways to straighten the rule of law in challenging times.

2. The Problem of The Rule of Law During the Pandemic

The rule of law entails a broad scope of principles such as accountability to laws that are publicly promulgated, equally enforced and independently adjudicated which are in accordance with international human rights standards.[432] Consequently, during the COVID-19 crisis the Secretary General of the Council of Europe, Marija Pejčinović Burić, explicitly said: 'The virus is destroying many lives and much else of what is very dear to us. We should not let it destroy our core values and free societies.'[433] Accordingly she sent to all members of the Council of Europe guidelines[434] that covered conditions of derogations with regard to human rights and respect of the rule of law. In times of crisis, it is of great significance to support cooperation between States in order to preserve these fundamental principles. In fact, the most difficult role for all States in 2020 was to establish fair balance between the public interest and individual rights. In this regard, the authorities must comply with 10 established principles in a case of emergency: legality, necessity, proportionality, non-discrimination, time-limits, non-derogable rights, international obligations, parliamentary scrutiny, effective remedy and transparency.[435] Indeed, in emergency situations States may impose restrictions in order to tackle the crisis and protect public health. Nevertheless, the Governments' actions are subjected to some boundaries even in times of crisis. This is the reason why the above mentioned principles are guaranteed in national legislation as

[432] United Nations Security Council, 'The rule of law and transitional justice in conflict and post-conflict societies' (S/616, 2004) 4.
[433] Council of Europe, 'Coronavirus: guidance to governments on respecting human rights, democracy and the rule of law5' (8 April 2020)
<https://www.coe.int/en/web/human-rights-rule-of-law/-/coronavirus-guidance-to-governments-on-respecting-human-rights-democracy-and-the-rule-of-law> accessed 1 October 2021.
[434] Council of Europe, 'Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis A toolkit for member states' (SG/Inf, 2020).
[435] Advocates for International Development (A4ID), the Bingham Centre for the Rule of Law, the University of Edinburgh Global Health Academy, 'The rule of law in times of health crises' (published 2020) 17-21.

well as in international treaties. For instance, all members of the Council of Europe have ratified and implemented in their national law the European Convention of Human Rights (ECHR). During the health crisis many claims of violations occurred under Articles 8, 10, 11 of the ECHR.[436] Despite the fact that the provisions of these Articles, in particular in the second paragraphs, impose situations in which the States may interfere, their actions are not unconditional. It is stated in a Venice report that even in situations of public emergency the principle of the rule of law should prevail and no-one should be put to trial before a court unlawfully.[437] Unfortunately, the COVID-19 virus had a negative impact on society, namely vulnerable groups, due to their socioeconomic and health status. Therefore, the pandemic has amplified the divide in societies on the ground of inequality. In reality, however, the preservation of international law standards, including the rule of law, 'not only helps justice, but also helps contain the spread of the pandemic itself.'[438] Logically, when the fundamental human rights are respected, institutions would further assert their legitimacy and people would be more inclined to follow States' orders and recommendations. However, the countries' measures in combating the Coronavirus drastically differ.[439] Authoritative regimes such as China, Singapore and Taiwan implemented stricter rules in comparison with democracies like Germany and Canada. In fact, 'authoritarianism does not guarantee an effective response, as the experience of Iran, which has endured a high rate of infection and a second wave of COVID-19, demonstrates'.[440] Undoubtedly, the pandemic had negatively influenced the whole world, but democracies have shown a better ability of adaptiveness and collaboration. 'Corporations, universities, foundations and non-profit organisations are cooperating and innovating with local authorities and internationally, whether to deliver medical relief and social support or to secure a vaccine.'[441] The rule of law has a central position in combating the Covid virus, but States must implement mechanisms of its protection.

3. Threats to the Rule of Law

Emergency situations do not, in theory, violate the rule of law, although they create an

[436] ECtHR, 'Factsheet – COVID-19 health crisis' (published 2021).
[437] European commission for democracy through law (Venice commission), 'Compilation of Venice commission opinions and reports on states of emergency' (CDL-PI003-e, 2020) 5.
[438] World Justice Project, 'Fundamental Rights and the COVID- 19 Pandemic' (published 2020) 13.
[439]See International Center for Not-for-Profit Law, 'COVID-19 Civic Freedom Tracker' <https://www.icnl.org/covid19tracker/?location=&issue=2&date=&type=> accessed 30 September 2021.
[440] Advocates for International Development (n 435), 37.
[441] Robin Niblett and Leslie Vinjamuri, 'Op-Ed: Why democracies do better at surviving pandemics' (Los Angeles Times, 26 May 2020) <https://www.latimes.com/opinion/story/2020-05-26/democracies-autocracies-coronavirus-pandemic-response> accessed 30 September 2021.

environment where the safeguards are more critical and difficult to uphold.[442] Broadly, we may identify two main groups of threats to the rule of law: threats directed at institutions and others in relation to human rights.[443] In the context of the first group, in order to impose COVID-19 restrictions the Governments may unnecessarily concentrate the power in the executive branch. This may lead to abuse of power, which is a serious threat to democracy. For example, around 16 people were killed by security officers in Ethiopia following protests against the arrests of local leaders and activists, allegedly for holding a meeting in contravention of COVID-19 restrictions.[444] In the Dominican Republic 85,000 people were detained in a three-month period for allegedly not following the curfew.[445] Furthermore, the Coronavirus has impacted the functioning of parliaments. Some countries such as France in 2020 had reduced the number of its meetings and were holding them remotely, while Germany continued to sit the meetings in person, but with fewer Members.[446] The crisis may, therefore, lead to postponed legislation and less transparency which infringes core features of the rule of law. Moreover, many elections were postponed due to the Coronavirus.[447] Delaying elections in times of crisis is inherently lawful, however States must not abuse their interference, for instance, by extending the time period unreasonably. Besides the legislature, the courts are also negatively impacted. For example, family courts have struggled to keep up with cases.[448] Even though some courts have transferred their trial to 'hybrid' hearings, held remotely and in person, the backlog of cases was still unbearable. As a result, some families had to wait months for courts' rulings. In particular, an urgent children matter 'had a hearing listed for six months later.'[449] Furthermore, the distribution of medical supplies and providing economic support have opened new opportunities for corruption. Consequently, the increased levels of fraud may lead to decreased legitimacy of institutions. As a

[442] Advocates for International Development (n 435), 22.
[443] ibid, 23.
[444] Amnesty International, 'Governments and police must stop using pandemic as pretext for abuse' (17 December 2020) <https://www.amnesty.org/en/latest/press-release/2020/12/governments-and-police-must-stop-using-pandemic-as-pretext-for-abuse/> accessed 1 October 2021.
[445] Amnesty International UK, 'COVID-19: Authorities commit human rights abuses in 60 countries under pretext of controlling pandemic - new report' (17 December 2020) <https://www.amnesty.org.uk/press-releases/covid-19-authorities-commit-human-rights-abuses-60-countries-under-pretext> accessed 29 September 2021.
[446] Inter-Parliamentary Union, 'Country compilation of parliamentary responses to the pandemic' (first published 25 March 2020) <https://www.ipu.org/country-compilation-parliamentary-responses-pandemic> accessed 1 October 2021.
[447] The International Institute for Democracy and Electoral Assistance (International IDEA), 'Global overview of Covid-19 impacts on elections' (20 December 2021) <https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections> accessed 29 September 2021.
[448] Michael Goodier, 'Justice, delayed: How Covid-19 exposes our crumbling courts system' (The New Statesman, 12 February 2021) <https://www.newstatesman.com/politics/uk-politics/2021/02/justice-delayed-how-covid-19-exposes-our-crumbling-courts-system> accessed 1 October 2021.
[449] ibid.

result, this will decrease public trust in institutions, which interferes with the rule of law.

In relation to the second group exposed to risks, the human rights issues, 'three rights are at the frontline in the current pandemic': the right to life and the duty to protect life, the right to health and access to health care and the freedom of movement. [450] In respect of the right to life all Members of the Council of Europe have the positive obligation to protect the lives of everyone within their jurisdiction. The right to life is an absolute right and it cannot be derogated even in times of crisis. Furthermore, the States' positive obligations under Article 2 include implementing effective legal framework and to conduct lawful investigations. Additionally, the right to health access and health care is inherent to the right of life. It imposes the obligation to protect the right of access to health facilities, goods, and services on a non-discriminatory basis, especially for vulnerable or marginalized groups.[451] In the UK the Government faced great difficulties with complying with this obligation. Due to the fact that the 'access to primary health care in the UK was severely disrupted'[452], it resulted in suspension of necessary surgical procedures for at least three months. In addition, the States had to restrict the freedom of free movement with the view to reducing the spread of the virus. Nevertheless, the interference must be lawful, proportionate and necessary in a democratic society. Unfortunately, some States are alleged to have abused these principles which directly violated Article 5[453] of the United Nations' Declaration. For instance, the president of the Philippines publicly stated that lockdown violators could be shot.[454] In Brazil citizens are bound by their feet for quarantine violation.[455] In countries like India and Pakistan the police used tactics of public shaming for people who breach lockdown which include physical beating or being subjected to public humiliation by being forced to crawl.[456]

All of the above mentioned examples in the two broad spheres of threats to the rule of law further manifest the need to effectively ensure guarantees against potential violations and abuses

---

[450] United Nations, 'COVID-19 and Human Rights We are all in this together' (published 2020) 4.

[451] Lisa Montel, Anuj Kapilashrami, Michel P. Coleman, Claudia Allemani, 'The Right to Health in Times of Pandemic: What Can We Learn from the UK's Response to the COVID-19 Outbreak?' (2020) 227 – 242 <https://www.hhrjournal.org/2020/11/the-right-to-health-in-times-of-pandemic-what-can-we-learn-from-the-uks-response-to-the-covid-19-outbreak/#_edn21 > accessed 28 September 2021.

[452] ibid.

[453] Article 5 of the Declaration by UN states that 'No one shall be subjected to torture or to cruel, inhuman or degrading treatment 05 or punishment.'

[454] CNBC, "Shoot them dead' — Philippine leader says won't tolerate lockdown violators' (2 April 2020) <https://www.cnbc.com/2020/04/02/philippines-duterte-threatens-to-shoot-lockdown-violators.html> accessed 01 October 2021.

[455] Juan Martinez, 'In Colombia, Citizens are Bound by Their Feet for Quarantine Violation' (9 April 2020) <https://riotimesonline.com/brazil-news/mercosur/in-colombia-citizens-are-bound-by-their-feet-for-quarantine-violation/> accessed 01 October 2021.

[456] TRT World, 'Why are police in the Indian Subcontinent humiliating quarantine violators?' (27 March 2020) <https://www.trtworld.com/magazine/why-are-police-in-the-indian-subcontinent-humiliating-quarantine-violators-34911> accessed 1 October 2021.

from the State.

4. Suggestions for Strengthening the Rule of Law in Times of Crisis

Despite the negative consequences from the Coronavirus that the whole world currently encounters, the 2030 Agenda for Sustainable Development (SDG) 16 still remains. Moreover, one of its main targets promotes the rule of law and ensures equal access to justice. The further establishment of the rule of law will promote great benefits in three major State sectors: economic stability, social sustainability and environmental sustainability.[457] Furthermore, the rule of law is of great significance in addressing and solving the COVID-19 situation. This legal principle entails an important aspect of the regulation of public relations between States and individuals. As mentioned, the rule of law is the bedrock of democratic societies which ensures effective and accessible justice, equality and respect for human rights. In this connection, the 'Rule of law and Covid-19 policy brief' makes eight suggestions for strengthening the rule of law: citizen participation, emergency restrictions anchored in the rule of law, fair laws for recovery, investments in justice services and legal aid, equitable justice innovation, alternative dispute resolution and informal justice in line with international standard, amplified justice for women and girls, a renewed spirit of multilateralism in alignment with the SDGs.[458]

First, promoting citizen participation in decisions that affect them directly will certainly increase legitimacy in public institutions. Additionally, when vulnerable groups are part of the decision-making processes, regarding their own health and safety, the response to COVID-19 would have a higher success rate eventually. Moreover, recently in South Africa projects in respect of legal literacy and knowledge have been organized.[459] This further manifests the need of educating basic legal skills in citizens with the view to achieving higher public trust in institutions. Second, in relation to emergency restrictions, they should be precisely defined in national provisions and in accordance with international law. In the presence of a well-defined legal framework less misinterpretations by officials will occur. Third, in the context of promoting fair laws for appropriate recovery, the enforcement of preventive measures in the legislation on the base of the country's economic and political level of development would increase the likelihood of tackling the next crisis. Fourth, States should make more investments in justice services, because when violations occur individuals should receive effective redress. Unfortunately, 'throughout the world, funding for legal programs and services, particularly for

[457] IDLO, 'Rule of law and Covid-19 Policy Brief' (2020) 4.
[458] ibid, 24-25.
[459] United Nations Development Programme, 'Legal literacy programmes'<https://www.undp-capacitydevelopment-health.org/en/legal-and-policy/enabling-legal-environments/legal-literacy-programmes/> accessed 1 October 2021.

low-income and vulnerable people is declining and in jeopardy, while income inequality, distribution of wealth and the cost of living all continue to grow.'[460] Fifth, in the light of the integration of equitable justice innovation, technological developments would improve the legal services significantly, reduce court's time periods and create better transparency for justice. Sixth, with regard to engaging in alternative dispute resolutions and customary and international standards, the main purpose of this suggestion is to ensure that everyone has access to justice. Seventh, in respect of the risks of gender-based violence, women and girls should have enhanced access to justice. For instance, the legal framework may include appropriate preventive measures in relation to psychological, social or legal services. Finally, the eighth suggestion proposes that in the light of the global challenges we face today, States should cooperate and support each other. The aim of this idea is to expand international communities and further assert their functions.

5. Conclusion

In conclusion, the rule of law is one of the milestones in a democratic society. One of its main aspects is the regulation of the relations between States and individuals. In the context of the Corona crisis, the rule of law was under great pressure from States' actions. Indeed, issues of public health and public safety should be highly considered, however the authorities' restrictive measures should not be a *façade* or incorporate strict and authoritarian actions. Moreover, the standards enshrined in the rule of law would benefit the COVID-19 response. Undoubtedly, in times of crisis cooperation is vital for solving crises between countries, but as well as between Governments and individuals.

[460] Lisa Moore and Trevor C.W. Farrow, 'Investing in Justice: A Literature Review in Support of the Case for Improved Access' (published 2019) 2.

CATÓLICA GLOBAL SCHOOL OF LAW

Católica Global School of Law was established in 2009 at the Law School of the Catholic University of Portugal and has become the center of the Católica's growing focus on international legal education.

Since its founding, **Católica Global School of Law** has been successful in achieving a series of goals: it has attracted a remarkable group of scholars and classes of graduate students, both coming from prestigious law schools from all over the world; it has launched three state of the art programmes (an **LL.M. Law in a European and Global Context,** an **Advanced LL.M. in International Business Law** and a **Global Ph.D. in Law**) and, responding the new market challenges and needs, will launch a new one for the academic year 2020-2021(**LL.M. in a Digital Economy**); and it is becoming an important center of graduate teaching and research in law from a global perspective in Lisbon. The quality of its programmes has been consistently recognized by international rankings, as well as the Financial Times, which selected **Católica Global School of Law** as one of the most innovative law schools in the world for six consecutive years.

The European Law Students' Association