



GESELLSCHAFT
FÜR FREIHEITSRECHTE

THE BUSINESS & HUMAN RIGHTS DIMENSION OF THE DIGITAL SERVICES ACT

STUDY BY ISABEL EBERT, MARIAM SHAKIL, ISABELLE
WILDHABER, ANDREIA DE OLIVEIRA

UNIVERSITY OF ST. GALLEN, SWITZERLAND

31 AUGUST 2023

Impressum

Gesellschaft für Freiheitsrechte e.V.

Boyenstr. 41

10115 Berlin

Telefon 030 549 08 10 – 0

Fax 030 549 08 10 – 99

info@freiheitsrechte.org

PGP/GPG Key ID FA2C23A8

Kontoverbindung

IBAN: DE 88 4306 0967 1182 9121 00

BIC: GENODEM1GLS

GLS Gemeinschaftsbank eG

Vertreten durch den Vorstand des Vereins

Dr. Ulf Buermeyer, LL.M. (Columbia)

Prof. Dr. Boris Burghardt

Prof. Dr. Nora Markard

Dr. John Philipp Thurn

Eingetragen in das Vereinsregister des Amtsgerichts

Berlin-Charlottenburg unter VR 34505 B (Satzung)

V.i.S.d.P.

Malte Spitz

Boyenstr. 41

10115 Berlin

Verfasst von



University of St.Gallen

gefördert durch

STIFTUNG
MERCATOR

Grafik und Layout

Berty Luyeye-Mbuka

Bernhard Leitner

Social Media

freiheitsrechte.org/newsletter

twitter.com/freiheitsrechte

chaos.social/@Freiheitsrechte

facebook.com/freiheitsrechte

instagram.com/freiheitsrechte

youtube.com/gesellschaft-fur-freiheitsrechte

linkedin.com/company/freiheitsrechte

TABLE OF CONTENTS

Table of Figures	6
Acknowledgements.....	7
Executive summary	8
Introduction and aim of this study	10
1. Business and Human Rights in the technology sector	10
1.1. Summary of the UN Protect, Respect and Remedy Framework and the UN Guiding Principles on Business and Human Rights.....	12
Pillar 1: The State duty to protect human rights	12
Pillar 2: The corporate responsibility to respect human rights	14
Pillar 3: Access to remedy for victims of human rights abuses	16
1.2. Regulating technology company conduct as part of the State Duty to Protect Human Rights.....	17
2. The Business & Human Rights dimension of the EU Digital Services Act (DSA) ..	21
2.1. Summary of the EU Digital Services Act (DSA)	22
2.2. Stakeholder Engagement as part of corporate compliance	25
2.3. Transparency requirements	27

2.4. Risk Assessment.....	31
2.5. Access to Remedy.....	34
3. Recommendations.....	38
References.....	42

TABLE OF FIGURES

Figure 1: Overview of relevant UNGPs and DSA provisions (non-exhaustive)	5
Figure 2: The three pillars of the UNGPs (source: OHCHR B-Tech 2020)	6
Figure 3 The Human rights due diligence process (source: OHCHR B-Tech 2020)	7

TABLE OF FIGURES

Figure 1: Overview of relevant UNGPs and DSA provisions (non-exhaustive)	5
Figure 2: The three pillars of the UNGPs (source: OHCHR B-Tech 2020)	8
Figure 3 The Human rights due diligence process (source: OHCHR B-Tech 2020)	10

ACKNOWLEDGEMENTS

We are deeply grateful to all those who played a role in writing this study. We would like to thank Asha Allen, Serge Biggoer, Elonnai Hickok, Lisa Hsin, Julian Jaurisch, Jason Pielemeier, Eliska Pirkova, Ben Shea and Florian Wettstein for their invaluable input and support throughout the research process, as well as Gesellschaft für Freiheitsrechte e.V. for making this study possible.

EXECUTIVE SUMMARY

This study discusses the Business and Human Rights Dimension of the EU Digital Services Act (DSA). The Business and Human Rights (BHR) framework is centred around the UN Guiding Principles on Business and Human Rights (UNGPs, 2011). These principles re-emphasize the State duty to protect human rights as enshrined in international human rights law and conceptualize the corporate responsibility to respect human rights, as well as access to remedy for victims of corporate human rights abuses. This study does not provide a holistic critique of the DSA in its entirety. Rather, this study analyses elements found within the DSA regulation that strongly resonate with the BHR perspective, and thereby, the UNGPs.

The DSA mirrors core elements of the UNGPs when it comes to assessing risks, providing transparency about platform governance, and engaging with stakeholders around corporate practices. The legislative text has been adopted in November 2022 and has often been labelled as an "adaptive" regulation. The effectiveness of its implementation will be dependent on the secondary legislation following in the Delegated Acts, as well as the rigor of enforcement by the regulator and the compliance by the companies when it comes to, inter alia, ensuring risk assessment practices.

The first part of this study (1.) introduces the core concept of Business and Human Rights, and its relevance in the technology policy arena. This part provides an overview of the main requirements of the UNGPs when it comes to technology company conduct regulation. The second part (2.) connects the Business and Human Rights debate to the legislative text of the DSA and its current implementation phase, and how the provisions of the DSA relate to the UNGPs. It places an emphasis on stakeholder engagement (2.2.), transparency (2.3.), risk assessment (2.4.) and access to remedy (2.5.). In the third part (3.), key recommendations are set out to provide for an effective implementation of the DSA from a perspective of the UNGPs, particularly with regards to strengthening i) stakeholder engagement, ii) transparency, iii) risk assessment methodologies, and iv) access to remedy.

Focus Theme	Relevant UNGPs (Pillar 2 and 3)	Relevant DSA provisions	Recommendation
Stakeholder Engagement	UNGP 18, 19	Art. 12, 40, 45, 46, 48 Recital 90 VLOPs	<ul style="list-style-type: none"> <input type="checkbox"/> Ensure substantive stakeholder engagement <input type="checkbox"/> Issue further guidance on methodologies <input type="checkbox"/> Assess policy coherence of expectations in relation to other legislative processes at EU/intl. level
Transparency	UNGP 19, 20, 21	Art. 15, 24, 27, 37, 39	<ul style="list-style-type: none"> <input type="checkbox"/> Ensure disclosure in meaningful and informative format <input type="checkbox"/> Defined metrics and concepts clearly <input type="checkbox"/> Align enforcement architecture with UNGPs
Risk Assessment	UNGP 13, 15b, 17, 19, 24 (UNGP 11, 12, 18, 23)	Art. 34 Recital 3	<ul style="list-style-type: none"> <input type="checkbox"/> Clarity on what constitutes “systemic risk” <input type="checkbox"/> Elaborate further on prioritization of addressing risks (UNGP 24) <input type="checkbox"/> Provide quality criteria for a robust risk assessment process and methodology
Access to Remedy	UNGP 22, 29 (UNGP 28, 30, 31)	Art. 20, 21, 22	<ul style="list-style-type: none"> <input type="checkbox"/> Ensure alignment of complaint handling mechanism with UNGPs’ effectiveness criteria (UNGP 31) <input type="checkbox"/> Require transparency about decision-making process, including independent review by companies <input type="checkbox"/> Provide strengthened rules on the conduct of trusted flaggers

Figure 1: Summary of relevant UNGPs and DSA provisions (non-exhaustive)

INTRODUCTION AND AIM OF THIS STUDY

The development and deployment of digital products and services by technology companies is at present largely unregulated when it comes to preventing and mitigating adverse impacts on human rights. Until recently, the United Nations Guiding Principles on Business and Human Rights (UNGPs) have predominantly been the basis for voluntary efforts to identify, prevent, and mitigate harms related to digital technologies. Emerging company practice demonstrates the relevance of the UNGPs for regulatory measures efforts to acknowledge these voluntary efforts and build upon them. At the same time, several regulatory proposals targeting technology company conduct that are currently in the drafting or more advanced stages of negotiation in this context. The standards of such endeavours set varying expectations that technology businesses must meet. The UNGPs can lend a helping hand in providing an anchor and analytical lens for technology company regulation, and the EU Digital Services Act (DSA)¹ acts as a pertinent example of how the UNGPs can help inform regulations. The objective of the UNGPs in enhancing standards and practices in relation to Business and Human Rights (BHR) is aimed at achieving tangible results for affected individuals and communities.

This study provides a brief introduction into the field of BHR and its role in contemporary technology regulation, connecting the discourse around BHR to the core elements of the DSA regarding its design. The aim is not a comprehensive mapping of the DSA against the whole spectrum of the UNGPs. Rather we focus on the distinct features of the DSA that bear a strong resemblance to the character of the UNGPs when it comes to stakeholder engagement, risk assessment, transparency, and access to remedy. The UNGPs have undoubtedly set an international standard of how human rights ought to be protected with regards to corporate conduct. Therefore, the objective of this study is to showcase to which extent the provisions in the the DSA may relate to the UNGPs. Hence, this study does not analyse the entire DSA instead picks out the elements found within the DSA provisions that echo with the UNGPs.

1. BUSINESS AND HUMAN RIGHTS IN THE TECHNOLOGY SECTOR

The UN United Nations Protect, Respect and Remedy Framework (Framework) was a milestone in a decade-long debate within the UN about the responsibilities of the private sector towards

¹ Regulation 2022/2065, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). <http://data.europa.eu/eli/reg/2022/2065/oj>.

human rights.² The Framework was endorsed by key stakeholders after a year-long consultative process with a wide range of stakeholder groups, including civil society, academia, business associations, individual companies, and States. Emerging from this Framework is a set of principles that have become the authoritative standard for responsible business conduct globally: UNGPs, adopted unanimously by the UN Human Rights Council in June 2011, postulate the responsibilities of the private sector towards human rights and re-emphasize the State duty to protect human rights as laid out in international human rights law.³ The UNGPs form the centrepiece of contemporary discussion in the BHR field as the key framework of reference.

While the UNGPs are sector-overarching in nature, they have witnessed significant uptake in recent years in the public policy documents of technology companies, for example to identify, assess and mitigate downstream human rights impacts.⁴ Equally, the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (MNE Guidelines), first issued in 1976, cover all sectors, and consequently also apply to technology companies.⁵ Already since 2011, the MNE Guidelines are aligned with the UNGPs, which were last updated in June 2023 to expand a chapter on technology. These broad frameworks, the UNGPs and MNE Guidelines, are complemented and deepened by tech sector-specific principles and initiatives, such as the Global Network Initiative and its Principles on Freedom of Expression & Privacy, the Manila Principles on Intermediary Liability, and the Santa Clara Principles on Content Moderation.⁶ On a similar vein, at the level of the UN, the UN Human Rights B-Tech Project⁷ was launched in 2019 as a project at the United Nations Office of the High Commissioner for Human Rights with the goal of promoting the uptake of the UNGPs in the technology sector. This contemporary policy emphasis on responsible business conduct in the technology sector and the increased need for downstream human rights due diligence frames the context of this study.⁸

2 Ruggie, J. (2011). Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises (A/HRC/17/31 Human Rights Council. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf

3 OHCHR. (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. (HR/PUB/11/04). United Nations. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

4 OHCHR B-Tech. (2021). The Strategic Aspects of Business Respect for Human Rights Part One: Overview and Reflections on Current Practice. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2021-11/strategic-aspects-part-1.pdf>; OHCHR B-Tech. (2022). The Feasibility of Mandating Downstream Human Rights Due Diligence: Reflections from technology company practices. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/documents/issues/business/2022-09-13/tech-downstream-hrdd.pdf>.

5 OECD. (2023). OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. <https://doi.org/10.1787/81f92357-en>.

6 Global Network Initiative. (2017) GNI Principles on Freedom of Expression and Privacy: <https://globalnetworkinitiative.org/gni-principles/>; Manila Principles on Intermediary Liability. (2015). Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation. <https://manilapprinciples.org/#:~:text=Any%20liability%20imposed%20on%20an,not%20comply%20with%20this%20principle.>; Santa Clara Principles on Content Moderation. (2018). On Transparency and Accountability in Content Moderation. <https://santaclarapprinciples.org/>.

7 OHCHR B-Tech Project. (2019). B-Tech Project OHCHR and business and human rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/en/business-and-human-rights/b-tech-project>.

8 Ingrams, M. G. & Wilde-Ramsing, J. (2023). Updated OECD Guidelines reconfirm downstream application of due diligence. Cambridge Core Blog. <https://www.cambridge.org/core/blog/2023/06/12/updated-oecd-guidelines-reconfirm-downstream-application-of-due-diligence/>.

1.1. Summary of the Protect, Respect and Remedy Framework and the UN Guiding Principles on Business and Human Rights

The UN Protect, Respect and Remedy Framework lays the foundations for the UNGPs and outlines the State duty to protect against human rights abuses stemming from or being linked to company activities, and businesses' responsibility to respect human rights, and to provide remedies for individuals who have been harmed by business activities. The UNGPs transpose the Framework into 31 guiding principles, which are structured into three pillars that provide a framework for governments and businesses to protect and respect human rights. The three pillars are: 1. the State duty to protect human rights, 2. the corporate responsibility to respect human rights, and 3. access to remedy.



Figure 2: The three pillars of the UNGPs (source: OHCHR B-Tech 2020)

Pillar 1: The State duty to protect human rights

Pillar 1 highlights the duty of States to protect individuals from human rights abuses by third parties, including businesses. It includes the obligation of States to ensure that laws and regulations are in place to prevent and address human rights abuses and to hold businesses accountable for their actions, as well as voluntary measures, such as incentive-based instruments.

For example, UNGP 3 sets out that in meeting their duty to protect, States should:

(a) enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps;

(b) ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights;

(c) provide effective guidance to business enterprises on how to respect human rights throughout their operations;

(d) encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.

This paper emphasises the State duty to protect against human rights abuses by businesses, as highlighted in the UNGPs' Pillar 1, which reflect human rights obligations of States under international human rights law. States are required to adopt appropriate measures to prevent and address human rights abuses being linked to or stemming from corporate activities. States should also consider the "full range of permissible preventative and remedial measures, including policies, legislation, regulations and adjudication" (UNGP 1).

Hence, as a part of the State duty to protect, governments should use a "smart mix" of voluntary and mandatory measures, including incentive-based mechanisms, such as export credits schemes, as well as regulatory options, i.e., laws, to require companies to respect human rights.

"The State's duty to protect human rights includes protecting against human rights abuses involving technology companies. This is consistent with States' existing human rights obligations, as reaffirmed in the UN Guiding Principles on Business and Human Rights. But States should not, intentionally or otherwise, roll back human rights protections when fulfilling this duty".⁹

9 OHCHR B-Tech. (2021): Bridging Governance Gaps in the Age of Technology - Key Characteristics of the State Duty to Protect: <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf>, p.3.

Pillar 2: The corporate responsibility to respect human rights

Pillar 2 emphasizes the responsibility of businesses to respect human rights in their activities, including their operations, products, and services, as well as their relationships with stakeholders, such as employees, suppliers, and customers. In particular, UNGP 15 provides that business enterprises should have in place policies and processes appropriate to their size and circumstances, including:

- (a) a policy commitment to meet their responsibility to respect human rights;
- (b) a human rights due diligence process [emphasis added] to identify, prevent, mitigate and account for how they address their impacts on human rights;
- (c) processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

Therefore, Pillar 1 discusses State duties, and Pillar 2 deals with business responsibilities towards human rights, regulation, and human rights due diligence as part of corporate responsibility. Both Pillars are closely intertwined. Pillar 2 also covers the responsibility of businesses to establish or participate in operational-level grievance mechanisms. For example, companies may, through their business practices, be involved with human rights harms either directly or indirectly because of their business relationships with third parties. In other words, a company can cause, contribute, or be directly linked to human rights harms.¹⁰ Hence, Pillar 2 should be understood as guidance for policymakers when drafting regulation that expects companies to

¹⁰ OHCHR B-Tech. (2021): Access to Remedy and the Technology Sector: Basic Concepts and Principles <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>.

carry out human rights due diligence to identify, prevent, mitigate, and account for how they address their impacts, in line with the expectations set out in UNGP 15.

Human rights due diligence broadly consists of four steps, building on extensive stakeholder engagement:¹¹

1. Identifying and assessing impacts to gauge the nature and extent of human rights risks;
2. acting to prevent and mitigate risks to people, including via integration within internal functions and processes;
3. tracking of effectiveness of risk mitigation responses over time; and
4. appropriate communication of performance with respect to addressing human rights impacts.

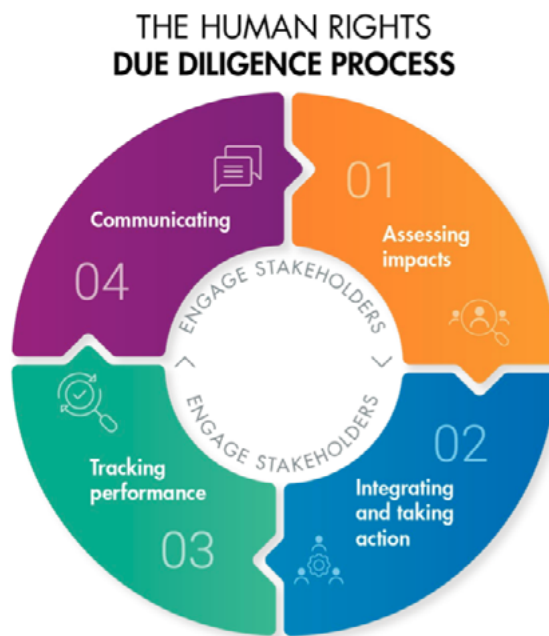


Figure 3 The Human rights due diligence process (source: OHCHR B-Tech 2020)

Also, businesses should implement or participate in mechanisms for access to remedy where harm has occurred stemming from or linked to business activities. Access to remedy is discussed in more detail in Pillar 3 of the UNGPs.

¹¹ OHCHR B-Tech. (2020). Key Characteristics of Business Respect for Human Rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/B-Tech/key-characteristics-business-respect.pdf>. For more information, please also view the report drafted by OECD. (2018). Due Diligence Guidance for Responsible Business Conduct. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf> and the recent update of the OECD MNE Guidelines (2023): <https://mneguidelines.oecd.org/targeted-update-of-the-oecd-guidelines-for-multinational-enterprises.htm>.

Pillar 3: Access to remedy for victims of human rights abuses

Pillar 3 recognizes the right of victims of human rights abuses to access effective remedies, including judicial and non-judicial mechanisms, for harm caused by business activities. It covers the obligation of States to ensure that such mechanisms are available and effective.

The UNGPs offer a framework for remedying human rights harms resulting from business practices that speaks to States, companies, investors, and advocacy organizations. Pillar 3 is grounded in the right to effective remedy, which is enshrined in international human rights law. Remedies for adverse human rights impacts of business activities can manifest in a range of forms, which warrant the adoption of several types of remediation mechanisms. As previously mentioned under Pillar 2, a company has the potential to cause, contribute or be directly linked to human rights harms. Hence, UNGPs 22 (Pillar 2) covers the responsibility of business to remediate. Pillar 3 covers the mechanisms that should be in place to make that happen and the ways in which they should be effective.¹²

Some human rights harms arising from company conduct can be directly dealt with by companies, for instance through operational-level grievance mechanisms. Such practices can also serve a preventative function in detecting potential adverse impacts. Other human rights harms might require different types of remedies, e.g., through courts.

The UNGPs divide mechanisms for seeking and delivering remedies for business-related human rights harms into three main types:¹³

1. “judicial mechanisms” (for example, domestic courts);
2. “State-based non-judicial mechanisms” (for example, mechanisms connected with the State which may have the potential to deliver remedies in some shape or form, such as regulators, ombudspersons, inspectorates, public complaints handling bodies,

¹² OHCHR B-Tech Project. (2021). Access to Remedy: Concept and Principles. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>.

¹³ OHCHR B-Tech Project. (2021). Access to Remedy: Concept and Principles. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>. p. 4.

National Contact Points for Responsible Business Conduct under the OECD Guidelines for Multinational Enterprises, and national human rights institutions);

3. “non-State-based grievance mechanisms” (for example, remediation mechanisms that are developed and administered by private entities such as companies or, in some cases, industry associations or multi-stakeholder groups).

Overall, the three Pillars of the UNGPs provide a comprehensive framework for governments to protect human rights and for businesses to respect human rights in the context of their business activities and provide appropriate remedies where harm has occurred.

1.2. Regulating technology company conduct as part of the State Duty to Protect Human Rights

It is widely acknowledged that international human rights law also applies to companies operating in the technology sector, and adverse human rights impacts stemming from or being linked to digital technologies.¹⁴ Digital technology plays a big role in modern society and impacts human rights and activities in pervasive and extensive ways. Technology regulation like all regulation should be consistent with international human rights law, where appropriate, with a particular emphasis on rights such as freedom of expression and privacy. The reason is that these rights are at the forefront of many recent harms stemming from or being linked to company conduct in the technology sector. Therefore, regulation of digital technologies and the conduct of companies developing, deploying, and using such technologies must be grounded in human rights law. The International Bill of Human Rights¹⁵ in combination with other core treaties¹⁶ form the legal framework of reference for human rights at the UN level. The UNGPs complement this legal framework and are widely regarded as “the most authoritative Statement of the human rights duties or responsibilities of States and corporations adopted at the UN level.”¹⁷ The series of consultations with stakeholder groups (business, governments, and civil society) that

14 Ebert, I., & Beduschi, A. (2022). Regulating business conduct in the technology sector: Gaps and Ways Forward in applying the UNGPs. <https://ore.exeter.ac.uk/repository/bitstream/handle/10871/129465/Regulating%20business%20conduct%20in%20the.pdf?sequence=1> p. 3.

15 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR); International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR); International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).

16 International Convention on the Elimination of All Forms of Racial Discrimination (adopted 21 December 1965, entered into force 4 January 1969) 660 UNTS 195 (CERD); Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW); Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85 (CAT); Convention on the Rights of the Child (adopted 7 March 1989, entered into force 2 September 1990) E/CN.4/RES/1990/74 (CRC); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (adopted 18 December 1990, entered into force 1 July 2003) A/RES/45/158 (CMW); International Convention for the Protection of All Persons from Enforced Disappearance (adopted 20 December 2006, entered into force 23 December 2010) A/72/280 (CPED); Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 3 May 2008) 2515 UNTS 3 (CRPD).

17 De Schutter, O. (2013). Foreword: Beyond the Guiding Principles. In: Deva, S. & Bilchitz, D. (eds.) Human rights obligations of business: Beyond the corporate responsibility to respect? Cambridge University Press, Cambridge, pp. xv-xxii.

accompanied the development of the UNGPs grant them unique authoritative and persuasive power.¹⁸

“The UNGPs are a powerful tool for guiding technology company conduct because they are internationally agreed and supported by a diverse set of stakeholders including business, governments and civil society around the world.”¹⁹

The State duty to protect human rights includes protecting rights holders, such as users and non-users, from adverse impacts of tech business activities. The UNGPs provide a useful roadmap for governments in addressing technology-related human rights issues, and in requiring technology companies to respect human rights. Through a “smart mix” of measures, the State has a critical role in ensuring responsible corporate conduct, facilitating multi-stakeholder engagement, and in driving corporate responsibility through measures that foster the uptake of human rights due diligence among technology companies.

As such, regulating business conduct through mandatory measures is part of this “smart mix” of measures. By implementing the DSA (as part of the larger Digital Services Act Package),²⁰ the European Union is currently paving the way for a large regulatory framework on technology company conduct. This development is reviving the discussion about the role of human rights in the digital age and in the use of digital technologies. Moreover, the DSA incorporates human rights protection and safeguards, by which it potentially advances content governance law through accountability rules. The DSA provides an interesting insight into how fundamental rights can be conceptualized in a regulatory framework governing technology company conduct. The UNGPs are essential in informing DSA enforcement, especially since the DSA specifically addresses the fundamental rights of users.

The present study analyses the extent to which BHR principles relating to stakeholder engagement, transparency, risk assessment, and access to remedy are mirrored in the DSA regulatory regime. This study deals with both the reporting obligations, which are intended to create more transparency about negative effects on fundamental rights, and the substantive obligations to protect fundamental rights.

1.3. Key requirements for technology regulation through the lens of the UNGPs

From a UNGPs’ perspective, technology regulation should align with the principles of human rights and emphasise business responsibility to respect human rights.²¹ As previously stated,

18 Wolfsteller, R., Li, Y. Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness. Hum Rights Rev 23, 1-17 (2022), p. 3-4.

19 OHCHR B-Tech Project. 2020. The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>.

20 European Commission. (2023). Shaping Europe’s digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

21 OHCHR. (2021). Guiding Principles on Business And Human Rights At 10: Taking stock of the first decade. (A/HRC/47/39). UN Working Group on Business and Human Right. <https://>

the UNGPs provide a framework for businesses to identify, prevent, mitigate, and remedy human rights impacts associated with their operations, products, and services, and are widely recognised as the authoritative international standard for responsible business conduct, along with the OECD MNE Guidelines. In this section, we discuss the main requirements for technology regulation according to the UNGPs.

In line with the UNGPs, the regulation of technology company conduct should uphold and protect human rights, as defined by international human rights law, including but not limited to the right to privacy, freedom of expression, and non-discrimination. States have a positive obligation to protect human rights against abuses by private actors. This means States need to ensure that digital technology should not be developed, deployed and/or used in a way that adversely impacts human rights, and regulatory measures should be in place to prevent such abuses stemming from or being linked to corporate conduct. The businesses that produce or use digital technology are subject to human rights responsibilities in line with the UNGPs and may in addition be subject to hard law obligations pertaining to, e.g., national laws. Yet, many current legal and regulatory frameworks have extensive blind spots when it comes to providing for rights-respecting corporate conduct in connection with digital technologies. New regulations introduced to address human rights in the technology sector can build on existing frameworks and good practices introduced by the UNGPs, such as the human rights due diligence concept, by leveraging the existing discussion on corporate responsibility to respect. Equally, regulations need to be periodically reviewed to validate adequacy and to amend provisions of regulations to adapt to emerging tech.

One of the main elements indicated by the UNGPs to assure human rights protection is corporate respect for human rights. Within the technology sector, adverse human rights impacts can occur while technological products are being manufactured (e.g., physical goods), but equally also during their deployment and end-use (e.g., digital services). That is why the full value chain is in scope of the UNGPs. Technology regulation must work in tandem by focusing on the corporate entity behind the technology being used, developed, and deployed. This requires companies to adopt a policy commitment to respect human rights, to carry out human rights due diligence to identify, prevent, and mitigate any adverse human rights impacts of their technologies. This includes assessing the potential risks associated with the development, deployment, and end-use of digital technologies and taking appropriate measures to address those risks, track their effectiveness and communicate about adopted measures. Equally, technology companies should put in place or contribute to access to remedial measures related to potential harm occurring

from or being linked to their business activities, such as through company-based operational grievance mechanisms, mediation, allowing victims to access independent legal advice.

Important design features for regulatory bodies in drafting regulation through a UNGPs perspective include²²:

- A broad view on human rights (all human rights need to be considered when conducting human rights due diligence);
- consistent application of the human rights due diligence terminology: expectations towards human rights due diligence to be conducted across all businesses and relationships, risks assessment methodologies and mitigation measures;
- value chain focus across the full business sphere (i.e., both upstream/supply chains and downstream);
- accompanying measures, such as incentive-based policy instruments, and enforcement provisions;
- process-oriented character of the legislation relating to the expectations towards businesses to meet (legislation should focus on regulating systems and processes deployed by companies);
- meaningful stakeholder engagement;
- measures enabling easy and direct access to effective remedy and redress, including appeal procedures.

Current technology development is complex, fast, and scaled by a globalised economy. Considering this, the UNGPs acknowledge the notion that in this highly networked environment, top-down regulation alone is not sufficient.²³ Therefore, technology regulation must be flexible and be suited to adequately identify, address and mitigate negative impacts on fundamental rights, stemming from business models, among others, criticized for surveillance based advertisement, manipulative practices via dark patterns, inherent lack of transparency, and poor access to effective remedy. Equally, regulation should promote meaningful and inclusive engagement of all relevant stakeholders, including but not limited to governments, civil society organizations, affected communities such as marginalized groups. Stakeholders should have

22 Ebert, I., & Beduschi, A. (2022). Regulating business conduct in the technology sector: Gaps and Ways Forward in applying the UNGPs. <https://ore.exeter.ac.uk/repository/bitstream/handle/10871/129465/Regulating%20business%20conduct%20in%20the.pdf?sequence=1>.

23 OHCHR B-Tech Project. 2020. The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>, p. 3.

the opportunity to provide input, raise concerns, and participate in decision-making processes related to technology.²⁴

Lastly, regulation of technology companies and by extension technology regulation should adopt a proportionate and human-centric approach, considering the potential benefits and risks of technology, and ensuring that the rights and well-being of groups and individuals are at the centre of regulatory measures, while a more flexible system, outlined by the UNGPs, can facilitate innovative activity based on rights-respecting conduct.²⁵

2. THE BUSINESS & HUMAN RIGHTS DIMENSION OF THE EU DIGITAL SERVICES ACT (DSA)

The DSA is an important piece of legislation in the field of digital technologies and platform governance, and of great interest from a UNGPs' perspective. Its main goal is to create a safer digital space in which the fundamental rights of recipients of the service are protected while still facilitating innovation.²⁶ The DSA came into force on 16 November 2022 and will be directly applicable across the EU in the first quarter of 2024. However, by February of 2023, online platforms²⁷ were called to disclose the number of active users. Platforms and search engines with at least 45 million users (10% of the population of the EU) have been designated as Very Large Online Platforms or Very Large Search Engines (VLOPs and VLOSEs, respectively).²⁸ These services will be subject to providing the European Commission (EC) with their first annual risk assessments by August 2023. By February 2024, EU Member States must appoint their Digital Services Coordinators, and platforms with less than 45 million users will also need to comply with the new regulations.²⁹

The combination of the DSA and the EU Digital Markets Act (DMA) with the EU General Data Protection Regulation (GDPR) provides an important regulatory framework containing essential safeguards for freedom of expression and privacy. The DSA contains several essential human rights-protecting provisions regarding due process and content moderation. All providers of intermediary services regulated by the DSA are obliged to respect the EU Charter of Fundamental Rights. This applies to platforms' terms and conditions,³⁰ or the development of new services

24 See e.g., Suzanne Vergnolle. (2023). Putting Collective Intelligence to the Enforcement of the Digital Services Act. <https://dsa-enforcement.vergnolle.org/>

25 Pelkmans, J., & Renda, A. (2014). How can EU legislation enable and/or disable innovation. European Commission, p. 1, 5.

26 DSA, Recital 9 and Pop, F. (2022, September 6). The Digital Services Act: Creating accountability for online platforms and protecting users' rights? EIPA. <https://www.eipa.eu/blog/the-digital-services-act-creating-accountability-for-online-platforms-and-protecting-users-rights/>.

27 DSA, Article 3 (i) defines "online platforms" as: "[...] a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".

28 See section 2.1. for more information on VLOPs and VLOSEs.

29 European Commission. (2023). Shaping Europe's digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

30 DSA, Article 14(4).

that will have to be compatible with the EU Charter.³¹ This is the first time such an obligation has been implemented. Some of these provisions are at risk of being undermined by sector-specific regulations that are meant to compliment the DSA, but not alter it. For example, such policy coherence questions arise regarding sector-specific regulations, that could imply carve-outs based on concrete categories of the content, e.g., terrorist content regulation.³²

The DSA features several requirements that speak to central components of the main goals of the UNGPs and their application in the field of technology company regulation more widely. Part 2. of this study will cover the aspect of BHR in relation to the DSA. To begin with, Section 2.1. of this study offers a concise overview of the DSA outlining its purpose, target audience, and primary objectives. Subsequently, Sections 2.2.-2.5. analyse various key aspects of the DSA regulation through the lens of the UNGPs, incorporating the key requirements of the UNGPs, as previously presented in Section 1.3. of this study. An emphasis will be placed on stakeholder engagement as part of company compliance (hereafter 2.2.), transparency requirements (hereafter 2.3.), risk assessment provisions (hereafter 2.4.), and access to remedy (hereafter 2.5.).

2.1. Summary of the EU Digital Services Act (DSA)

The DSA is a European Union legislation that establishes a comprehensive regulatory framework for providers of digital intermediary services, which will have direct applicability throughout the EU. Its main objective is to create a safer, more transparent, predictable, and accountable internet for users of such services by defining and obligations on their design, operations, and procedures (in DSA language “systems and processes”). The DSA establishes a set of rules and processes, around how content is moderated and disseminated. Recital 47 explicitly says that “all providers of intermediary services should also pay due regard to relevant international standards for the protection of human rights, such as the United Nations Guiding Principles on Business and Human Rights.” The DSA implements mechanisms to combat illegal content, products, and services online.³³ It also provides procedural safeguards for users whose content is removed

31 DSA, Article 34(1)(b). By which VLOPs and VLOSEs must conduct risk assessment before deploying new services that are likely to have any actual or foreseeable negative impact on the exercise of fundamental rights.

32 Article 19. (2020 April 7). EU: Terrorist Content Regulation must protect freedom of expression rights. <https://www.article19.org/resources/eu-terrorist-content-regulation-must-protect-freedom-of-expression-rights/>; And: La Quadrature du Net (LODN). (2022 March 9). French deputies must reject online censorship without a judge in one hour. <https://edri.org/our-work/french-deputies-must-reject-online-censorship-without-a-judge-in-one-hour/>; And: Rojszczak, M. (2022). Online content filtering in EU law—A coherent framework or jigsaw puzzle?. *Computer Law & Security Review*, 47, 105739.

33 DSA, Article 9.

or otherwise restricted by platform providers,³⁴ and requires legally mandated transparency criteria, including regarding terms and conditions³⁵ and algorithmic recommender systems.³⁶

The DSA covers intermediary services established in the EU as well as those based outside of it, if they provide services in the EU single market.³⁷ Intermediary services are defined as digital services that allow users to store, access and share information online,³⁸ such as internet access services, cloud services, online marketplaces, rental platforms, search engines, “app” stores, social networks, or content-sharing platforms.³⁹ All online intermediaries must comply with several new transparency obligations to increase accountability and oversight.⁴⁰ Besides this baseline, further provisions apply, in layers, to certain types of providers.⁴¹ Bigger and more socially significant services must fulfil proportionally stricter obligations, such as the aforementioned VLOPs and VLOSEs.⁴² Due to their reach, VLOPs and VLOSEs are considered particularly important to the facilitation of public debate, economic transactions and the dissemination of online information to the public.⁴³ Therefore, the DSA considers it necessary to impose additional obligations on the providers of those platforms beyond those applicable to all online platforms.⁴⁴

VLOPs are the largest and most influential online platforms operating within the EU. In April 2023, the Commission adopted the first designation decisions under the DSA, designating 17 VLOPs and 2 VLOSEs that reach at least 45 million monthly active users.⁴⁵ VLOSEs, on the other hand, are search engines that have a significant impact on the functioning of the internal market of the European Union, such as Google and Bing. VLOPs’ and VLOSEs’ additional obligations include requirements to provide clear information about their algorithmic systems⁴⁶ to

34 DSA, Article 10.

35 DSA, Article 14.

36 DSA, Article 27.

37 DSA, Article 2(1). And: Bedi, I. (2023 February 20). The Territorial Scope of the EU Digital Services Act: Isaac Bedi considers the territorial scope of the EU Digital Services Act and how it will apply to organisations outside of the EU. Burges-Salmon. <https://www.burges-salmon.com/news-and-insight/legal-updates/technology-and-communications/the-territorial-scope-of-the-eu-digital-services-act#:~:text=What%20is%20the%20territorial%20scope.in%20a%20world%20without%20borders>.

38 DSA, Article 3(g).

39 European Broadcasting Union (EBU). (2023). Digital Services Act: A Handbook For Public Service Media. EBU Legal and Policy. <https://www.ebu.ch/files/live/sites/ebu/files/Publications/Reports/open/10022023-Digital-Services-Act-Handbook%E2%80%93Public-Version.pdf>, p. 4.

40 European Commission. (2022 November 16). Digital Services Act: EU’s landmark rules for online platforms enter into force. EC Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906.

41 Clifford Chance. (2022). The digital services act: what is it and what impact will it have?. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/the-digital-services-act-what-is-it-and-what-impact-will-it-have-updated-december-2022.pdf>, p. 4.

42 DSA, Article 33.

43 DSA, Recital 75.

44 DSA, Recital 75.

45 The 17 listed companies are: VLOPs: Alibaba AliExpress, Amazon Store, Apple AppStore, [Booking.com](https://www.booking.com), Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando; VLOSEs: Bing, Google Search. These platforms have been designated with reference to their user data at 17 February 2023.

46 DSA, Article 40(1) and (3).

implement measures to prevent the spread of illegal content,⁴⁷. All online platforms, not only VLOPs/VLOSEs, need to establish effective redress mechanisms for users.⁴⁸

The DSA marks a new direction in EU digital policy. Alongside the DMA, resembling the regulatory approach taken in EU competition law, the DSA allows the EC to request all relevant information from companies to carry out its duties, regardless of ownership, location, format, or storage medium.⁴⁹ The oversight of the VLOPs will be centrally governed at the EC. The legislative text around the supervisory powers is aligned with Regulation 1/2003 concerning EU competition law. The new EU digital policy direction builds on key goals of the GDPR in terms of a responsible internet ecosystem, yet identifies a significant departure from the GDPR approach. As many platforms operating in the EU have their EU subsidiary in the jurisdiction of Ireland, the Irish Data Protection Authority has become to a certain extent a bottleneck for enforcement of the GDPR.⁵⁰ These lessons learned from the GDPR enforcement process were integrated into the new DSA model with the division of tasks between national regulators, the EC, and the newly established European Board for Digital Services to oversee and monitor the implementation and enforcement of the (that mixes regulators and EC). This is to be further clarified over the remaining months of 2023, as well as in practice.

Independent oversight, as well, is a critical element of any regulatory framework, as it provides an external check on the actions and decisions of the entities subject to the regulation. In the context of the DSA, independent oversight is particularly important given the significant impact that online service providers can have on individuals' fundamental rights and on society collectively. Addressing the importance of independent oversight, the DSA includes provisions to establish an EU Board of the DSA.⁵¹ Furthermore, the DSA includes provisions for independent oversight of online advertising, and it expands the existing GDPR protections against profiling and further restricts targeted advertising.⁵² Article 26 of the DSA requires online platforms to establish independent oversight mechanisms to monitor compliance with the DSA's rules on online advertising, including transparency and disclosure requirements.⁵³

In line with the UNGPs, the DSA puts an emphasis on regulating systems and processes deployed by the corporate entity rather than the technology per se, yet the corresponding systems and processes rely on technical functionalities, products and features used for content moderation, curation and/or advertising. What the DSA does not do is singling out concrete categories of

47 DSA, Article 34.

48 DSA, Article 14(5).

49 Dietrich, M., Jung, N., and van Rooijen, A. (2022 November 25). Digital Regulation in Europe. Global Competition Review. Digital Markets Guide – Second Edition. Global Competition Review. <https://globalcompetitionreview.com/guide/digital-markets-guide/second-edition/article/digital-regulation-in-europe>.

50 ICCL. (2023). 5 years: GDPR's crisis point ICCL report on EEA data protection authorities. <https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf>.

51 DSA, Section 3.

52 Van den Brande, B. (2022 November 7). The Digital Services Act has been approved: targeted advertising will soon be restricted. Lexology. <https://www.lexology.com/library/detail.aspx?g=cefceeff-6426-4c2c-8cec-b45cae3381b8>.

53 See: DSA, Article 26 (advertising on online platforms), Article 27 (recommender system transparency), Article 28 (online protection of minors), Article 37 (independent audit), Article 38 (recommender systems), Article 39 (additional online advertising transparency), and Article 42 (transparency reporting obligations).

illegal content. The incision point is corporate governance and the methods and measures to identify, address and mitigate risks.

2.2. Stakeholder Engagement as part of corporate compliance

Stakeholder engagement is a key element of the UNGPs and is critical for promoting respect for human rights in business practices (see UNGPs 18a, b, 20b, 21, 29, 31). Businesses can improve their practices to ensure that their operations respect human rights by meaningfully engaging with stakeholders throughout their human rights due diligence practices and developing effective remedy and grievance mechanisms. UNGP 18 asserts the importance of identifying actual or potential human rights risks stemming from a company's business conduct, whether it be a direct or indirect contribution. Stakeholders in this regard include human rights experts (i.e., civil society organisations or internal company human rights expert), who would ideally need to assist the company in assessing the human rights context prior to conducting any business activity (UNGP 18 (a)). Such measures would enable the company to gauge how human rights could be impacted, as well as identify who would be most negatively impacted based on the specific business activity. Once the company has established the potentially affected groups, UNGP 18 (b) guides companies to then involve such groups in meaningful consultations to further identify potential or existing risks, as well as to involve them in the design and development of risk mitigation measures. Human rights situations are dynamic; therefore, it is imperative that companies conduct human rights risk assessments and partake in meaningful consultations with relevant stakeholders at regular intervals.

Beyond identification of human rights risks, UNGP 20 (b) highlights that stakeholder engagement is equally necessary when verifying whether the human rights impacts are being adequately addressed by the company. This is to ensure that the affected groups can provide feedback on efforts taken by companies to mitigate human rights risks, and whether such measures are indeed adequate, or further actions are required. Stakeholder consultations can, according to the commentary of UNGP 21, be one of the ways with which companies can publicly communicate how they address human rights impacts. Once human rights infringements have occurred, companies contributing to or causing such harms have the responsibility to remediate victims. While remedy mechanisms are not the central focus of this section's discussion, it is nonetheless important to mention them. Stakeholder engagement is necessary to establish appropriate remedial mechanisms, with affected groups at the core (UNGPs 23, 28, 29, 30). As part of the 'effectiveness criteria', UNGP 31 guides companies to actively engage and have a

dialogue with relevant stakeholders to verify whether the proposed remedy mechanisms are adequately designed to address and resolve grievances.

The DSA proposes new rules and requirements for online platforms and services, aimed at promoting greater accountability,⁵⁴ transparency,⁵⁵ and respect for human rights.⁵⁶ To ensure effective implementation of these requirements, companies will need to engage with a range of stakeholders, including users, civil society organizations, and regulatory bodies. This is a lesson learned from the UNGPs' advocating consultations, as mentioned in Section 1.3. Recital 90 says VLOPs/VLOSEs "should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations."

The DSA contains several provisions that encourage collaboration between companies and civil society organizations. For example, the access to data framework stipulated in Article 40 is another mechanism for stakeholder engagement. This measure can potentially empower civil society organizations and their voice in the DSA enforcement process. Equally, Article 35(2) provides that the Commission may invite providers of such platforms and search engines, as well as other relevant stakeholders, including civil society organisations, to participate in drawing up codes of conduct and committing to specific risk mitigation measures. Article 37(3), on the other hand, allows for the involvement of Member States' authorities, Union bodies, offices, agencies, civil society organizations, and other relevant organizations in drawing up and testing crisis protocols to be applied in the event of significant systemic risk.

One of the roles of Digital Services Coordinators (DSCs) is to engage with stakeholders, such as online platforms, civil society organizations, and the public, to ensure that the DSA's provisions are met. As previously mentioned, the UNGP 20 (b) asserts the need for independent monitoring of measures taken by companies in mitigating potential and actual human rights risks. One of the functions of the DSCs is to act independently from other public authorities or private parties (Article 39), which allows them to engage with stakeholders in an impartial and fair manner, thereby enabling affected groups to provide feedback. They may conduct on-site inspections, interviews, and request data from platforms (Article 40), and it is important that stakeholders cooperate with the DSCs to ensure that DSA compliance is achieved. Also, the EU Board may help ensure that stakeholder engagement is comprehensive and effective.⁵⁷

In sum, the DSA provides for clear provisions that resonate with the BHR framework in terms of involving a variety of relevant stakeholders in a business' decision-making processes.

54 "[The DSA] will give better protection to users and to fundamental rights online, establish a powerful transparency and accountability framework for online platforms and provide a single, uniform framework across the EU." European Commission. (2023 April 25). Questions and Answers – Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348. Some measures that provide methods for accountability can be found on DSA, Article 37 (independent audit) and Article 40 (data access and scrutiny).

55 DSA, Article 42.

56 For example: DSA, Article 1, Article 14 (4), Article 34 (1) (b), Article 35 and Article 36.

57 Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12(4), 758-774. doi:10.1017/err.2021.8. p. 772.

Nevertheless, companies should be cognizant to not only undertake stakeholder engagement for the narrow purpose of compliance with the DSA, but should further intend to undertake meaningful stakeholder engagement for human rights due diligence as envisioned by the UNGPs as a strategic purpose of involving affected stakeholders across company functions. This can include working with civil society organizations, academics, expert advisors, multi-stakeholder initiatives and potentially affected stakeholders to identify areas of risk, consulting on policies and procedures, and sharing information about efforts to promote compliance (see UNGPs 18b, 20b, 21, 31). Companies should avoid creating siloed or stand-alone engagements solely for DSA compliance. Conversely, to ensure that DSA systemic risk assessments draw upon prior stakeholder engagement may create organizational synergies. Moreover, companies are not absolved of any accountability after having only engaged with relevant stakeholders, but are further required to be transparent about their actions, which the next section will elaborate on in more detail.

2.3. Transparency requirements

Human rights due diligence is a core component of transparency that the UNGPs refer to. Companies need to identify potential adverse impacts stemming from or linked to business activities and companies need to take action to address these impacts across relevant internal functions based on the severity of risks to the rightsholders (UNGP 19). Companies should continuously track the effectiveness of their proposed mitigation strategies based on appropriate qualitative and quantitative metrics, drawing upon expertise of internal and external stakeholders (UNGP 20). Businesses ought to communicate the results in a public manner to be in adherence to UNGP 21. The business needs to provide communication stemming from its own records as well as “when concerns are raised by or on behalf of affected stakeholders” (UNGP 21) are made against the company by affected groups. The effectiveness of the remedy mechanisms should also be shared externally through various forms, such as providing statistics, case studies, or more detailed information about the handling of certain cases (UNGP 31, see also section 2.5. on access to remedy).

Transparency is a critical aspect of the DSA that aligns with the UNGPs, particularly as part of conducting human rights due diligence.⁵⁸ The DSA requires companies to communicate transparently with stakeholders, including affected individuals and groups, and investors, consistent with the corporate responsibility to respect human rights as laid down in Pillar 2 of the UNGPs, mentioned above.⁵⁹ The first important transparency requirement relates to the **provision regarding terms and conditions**. Article 14 DSA establishes that providers of intermediary services must include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service,

⁵⁸ DSA, Article 21.

⁵⁹ DSA, Article 14(1).

in their terms and conditions. The providers of intermediary services must act in a diligent, objective, and proportionate manner in applying and enforcing the restrictions. Providers of VLOPs and VLOSEs must provide recipients of services with a concise, easily accessible, and machine-readable summary of terms and conditions. This is very important, as the terms and conditions are the main document establishing the contractual terms of the relationship between service providers and users.

The DSA also requires digital service providers to present **clear and transparent information about their content moderation policies, procedures, and practices**. This obligation is contained in Article 15, which mandates intermediary service providers to make publicly available easily comprehensible reports on their content moderation activities during the relevant period, at least once a year. These reports should include: i) information on the number of orders received from Member States' authorities; ii) the number of notices submitted; iii) information about content moderation activities initiated by the provider; and iv) the number of complaints received through internal complaint-handling systems. Online platforms must also include information on the number of disputes submitted to out-of-court dispute settlement bodies.

Similarly, Article 24 dictates the transparency reporting obligations for providers of online platforms with regards to the effectiveness of mitigation and remedy mechanisms. Information on out-of-court dispute settlements, such as the number of settlements, the average time required to complete such settlements, and the instances where the online platforms have implemented the decisions of the out-of-court settlement bodies, should be included in the reports. The DSA expects online platforms to track manifestly illegal activity occurring on their platforms and consequently suspend such users' accounts after having provided them with an initial warning (Article 23). Therefore, Article 24(1)(b) requires online platforms to report on an explanation of how they distinguished between suspensions enacted for the provision of manifestly illegal content, as well as under what circumstances unfounded warnings and unfounded complaints were deposited. The EC may further require online platforms and search engines to provide additional information, including explanations and substantiations in respect of the data used, which should not include personal data. As the DSA is an adaptive regulation, Article 24(6) grants the EC the right to adopt implementing acts that will provide templates regarding the form, content, and other details of reporting that online platforms and search engines will be obligated to adhere to.

As mentioned in Section 2.1., some heightened obligations are attributed to certain classes of digital providers. With that in mind, Article 37 of the DSA builds on the provisions of Article 15 by requiring **VLOPs and VLOSEs to undergo independent audits at least once a year** to assess compliance with Chapter III due diligence obligations, including commitments made under codes of conduct and crisis protocols. The audits will be conducted at the providers' expense, and the auditors will be granted access to all relevant data and premises necessary for the audit. Providers are also prohibited from hampering or unduly influencing the audit process. The

audit report and implementation report will be redacted and then published for transparency reporting purposes. Only the EC will be entitled to have full unredacted access to the reports.

Given the goals of the DSA to protect human rights, it is key to create transparency of advertising practices. In that regard Article 39 DSA requires VLOPs and VLOSEs to compile and make publicly available an **advertisement repository** containing information related to the advertisements presented on their interfaces. This repository should be accessible through a searchable and reliable tool, as well as application programming interfaces (also known as APIs). The repository must contain information such as the content of the advertisement, the natural or legal person on whose behalf the advertisement was presented, and the total number of recipients reached. The repository must not contain any personal data of recipients, and providers must make reasonable effort to ensure the accuracy and completeness of the information. Additionally, Recital 70 provides for greater clarity on the rights of the users of the recommender systems services. Online platforms should consistently ensure that users are appropriately informed about how such systems prioritise suggestive information for the users and which parameters are used to train the systems to make such prioritisations.

The topic of data collection and usage has garnered significant attention, particularly after the implementation of the GDPR. As previously mentioned, the UNGPs' importance of creating businesses that are built on respect for human rights has been mostly related to their traditional 'offline' practices. Therefore, the GDPR stands out as one of the first instruments that provides a concrete answer on how to practically incorporate a specific human rights aspect, such as online privacy and data protection, into technology companies' online operations.⁶⁰ The DSA, in Article 40, builds on this and establishes extensive provisions on how VLOPs and VLOSEs are required to provide **clear and transparent information about the data collection and use**. They must also provide relevant authorities with access to necessary data for monitoring and assessing compliance with the DSA. Requests for data access must be made within a reasonable period, and the accessed data may only be used for monitoring and assessing compliance with the DSA. This provision of the DSA complements the GDPR by establishing additional requirements for online platforms and search engines that process large amounts of data. In Article 40 DSA, providers of VLOPs and VLOSEs are required to provide clear and transparent information about the data they collect and how it is used. They must also provide access to data necessary for monitoring and assessing compliance with the DSA. Overall, Article 40 DSA reinforces the principles of transparency and accountability that are central to the GDPR but with a focus on data access for researchers, which will enable them to have better opportunities to study platforms. This thereby ensures that VLOPs and VLOSEs are obligated to share their data with researchers (which includes, for example, CSOs) in a transparent manner. Article 40(8) provides for clearer guidance on who is eligible as 'researchers': i) that the researcher is affiliated to a research organisation (i.e., university, library, research institute, or any other entity whose

60 Minović, A. (2022 August 7). GDPR: Integrating human rights into business practices. DIPLO. <https://www.diplomacy.edu/blog/gdpr-integrating-human-rights-business-practices/>.

primary goal is to conduct scientific research or to carry out educational activities),⁶¹ and ii) are independent of commercial interests. This provision is perhaps the most comprehensive one for researchers to date, as it provides access and contributes to accountability and transparency. Transparency rules focusing on recommender systems or online advertising, on the other hand, falls under Article 27, whereby VLOPs will be required to compile the data used for their displayed advertising and make it publicly available until one year after the advertisement was displayed.

This approach promotes accountability, whereas current existing regulatory initiatives and debates rely on limited data shared by companies, and the transparency exercises mandated by the DSA will be essential in enhancing the quality of norms and practices.⁶² The transparency obligations under the DSA might therefore promote the generation of valuable data, not just for the EU, but also for global policy discussions on holding platforms accountable and promoting best practices in risk due diligence. Meaningful transparency measures can foster a race to the top of rights-respecting practices and enable differentiation between industry leaders and laggards when it comes to responsible business conduct. The focus of the DSA on transparency is an essential feature and echoes well with UNGP 21 calling for “communication” as a means of “providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors”⁶³ as part of human rights due diligence. One of the ways that the EC can strengthen the DSA, however, is by defining what constitutes as ‘manifestly illegal’ content, as no such provision currently exists in the draft regulation, which is also relevant for the subsequent section 2.4. on risk assessment requirements in the DSA.

61 Definition found in Article 2 (1) of Directive (EU) 2019/790.

62 Clifford Chance. (2022). The digital services act: what is it and what impact will it have? <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/the-digital-services-act-what-is-it-and-what-impact-will-it-have-updated-december-2022.pdf>. p. 4-6. And: Singh, S. (2022 January 21). The EU's Digital Services Act Makes a Positive Step Towards Transparency and Accountability. But Also Raises Some Serious Questions. New America. <https://www.newamerica.org/oti/blog/the-eus-digital-services-act-makes-a-positive-step-towards-transparency-and-accountability-but-also-raises-some-serious-questions/>.

63 Ruggie, J. (2011). Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises. (A/HRC/17/31). Human Rights Council. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf. p. 244.

2.4. Risk Assessment

Human rights due diligence, as envisioned by UNGP 15 (b), is a process that aims at identifying, preventing, mitigating human rights infringements, while accounting for how such harms are addressed. According to UNGP 12, businesses have the responsibility to respect all internationally recognised human rights that are encoded in the International Bill of Human Rights,⁶⁴ along with the principles enshrined in the International Labour Organisation's Declaration on Fundamental Principles of Rights at Work.⁶⁵ When such businesses are also operating in conflict areas, they ought to respect the standards of International Humanitarian Law. Furthermore, UNGP 13 asserts that risk assessments should be conducted beyond a business's own operations and extend it to recognise the ways that their business conduct could, as well, indirectly impact human rights. In other words, human rights risk assessments should be conducted throughout the businesses' own actions and omissions (direct harms) and be aware of actual and potential human rights risks caused by other business relationships (indirect harms, i.e., entities in its value chain).

Being cognizant of the fact that businesses come in all shapes and sizes, the UNGPs assert that the level of due diligence requirements would differ depending on the complexity of the business itself (UNGP 17 (b)). Therefore, UNGP 17 instead expects that large companies at the minimum identify general areas where the risk of human rights violations are most significant and that they focus primarily on such areas. Nevertheless, it is equally important for businesses to acknowledge that conducting human rights due diligence in and of itself is insufficient in absolving themselves from liability.

The DSA hints at the scope, scale, and remediability as assessment criteria. VLOPs and VLOSEs must conduct risk assessments of their services according to Article 34. They must identify and mitigate any systemic risks regarding: (a) dissemination of illegal content; (b) negative effects on fundamental rights, civic discourse and public security; (c) foreseeable negative effects related to gender-based violence, and (d) protection of public health and minors, as well as serious negative consequences to personal physical and mental well-being. The risk assessment should be specific to the service, proportionate to the systemic risks, and consider relevant factors such as the design of recommender systems, content moderation systems, applicable terms and conditions, systems for selecting and presenting advertisements (advertisement repositories and ad-delivery techniques), and data-related practices as well as crisis response mechanisms. The risk assessments should also analyse how intentional manipulation of the service and amplification of illegal content may contribute to these risks. Providers must preserve supporting

64 UN General Assembly, International Bill of Human Rights, 10 December 1948, A/RES/217(III)A-E, available at: <https://www.refworld.org/docid/3b0f08b48.html>.

65 International Labour Organisation (ILO). (1988). ILO Declaration on Fundamental Principles and Rights at Work. <https://www.refworld.org/docid/425bbdf72.html>.

documents of the risk assessments for at least three years and provide them to the EC upon request.

Recital 83 of the DSA provides for clearer guidance on how VLOPs and VLOSEs can assess systemic risks. These providers should concentrate on the systems or other components that may contribute to the risks. This includes all relevant algorithmic systems, particularly their recommender systems and advertising systems. Additionally, careful consideration should be given to related data collection and use practices. Along with evaluating their content moderation procedures, technical resources, and allotted resources, they should also determine whether their terms and conditions are suitably enforced. VLOP and VLOSE providers should pay attention to information that is legal but still contributes to the exacerbation of systemic risks. These service providers should pay closer attention to how misinformation or disinformation is spread or amplified via their services. They should appropriately account for this in their risk assessments in cases where algorithmic amplification of information increases the systemic risks. Moreover, risk assessments must take into consideration localised harms and linguistic variations. Recital 81 of the DSA points out clearer guidance on how VLOPs and VLOSEs can identify risks to children's rights. Such providers should take several factors into account when evaluating risks to children's rights, such as how simple it is for children to understand how online services are designed and how they operate. Furthermore, it is essential for providers to identify how easily children can be exposed to online content that could harm their health, physical integrity, and moral development. These dangers may be present, for instance, in the design of online interfaces that mistakenly or purposely prey on the vulnerability and inexperience of children or could lead to addictive behaviour.

The DSA's process-oriented risk assessment stipulations and requirements for due diligence align in their essential design with the UNGPs' perspective on human rights due diligence. Yet, there are some caveats, such as the DSA not explicitly using the term "human rights due diligence."⁶⁶ VLOPs and VLOSEs can implement the provisions for risk assessment of their services against systemic risks in line with the UNGPs. However, the legislative text of the DSA requires further strengthening. Delegated Acts are defined by the EU as "non-legislative acts that serve to amend or supplement the non-essential elements of the legislation". In other words, they serve as detailed assistance on how legislation should be interpreted. There is no delegated act in Article 34 of the DSA, only informal guidelines. Further clarity is needed as to how "systemic risk" relates to the UNGPs and to how companies ought to interpret the definitions of the "systemic risks". Such guidance could be included in guidelines developed by the EC, which can currently be found in Article 35 (mitigation of risks), but not in Article 34. It would be pertinent for the EC to outline both how to assess and mitigate risks. Furthermore, the identification of harms to children can be a slippery slope, considering there is no clear guidance on how children themselves should be consulted in order to appropriately identify children-

66 Holly, G. et. al. (2023). How do the pieces fit in the puzzle? Making sense of EU regulatory initiatives related to business and human rights. The Danish Institute for Human Rights. https://www.humanrights.dk/files/media/document/2023_06_02_EU-RegulatoryMeasuresExplainer_EN_june2023.pdf.

specific harms. Therefore, it is necessary for the EC to require VLOP and VLOSE providers to consult with experts that work at the intersection of children's and digital rights.⁶⁷

The DSA emphasises the importance of the EU Charter throughout its text, and it serves as a tool to promote its application online.⁶⁸ The significance of the EU Charter in governing online regulations is emphasized in Article 34 (1)(b), which singles out significant negative effect on fundamental rights. Equally, Recital 3 of the DSA emphasizes the crucial role of responsible conduct by digital service providers in enabling the protection and exercise of the fundamental rights ensured by the EU Charter. Further clarity is needed on how the concept of "systemic risk" relates to the international human rights framework and to ensure alignment with the UNGPs in the corporate response to complying with the DSA. The DSA's main text also does not provide sufficient detail on the expectations towards human rights risk assessment and the importance of assessing human rights risks related to platform activities for auditing purposes.

The DSA has the potential to harmonize efforts to incorporate human rights principles into content governance, based on existing international frameworks and coherent operation of companies in scope of the law across borders. Regulators could use the provisions on risk assessments and mitigation measures, such as codes and protocols, to reinforce existing standards and guidelines of entities already performing these assessments. Expert organizations can come together to create a global blueprint for meaningful risk assessments, leveraging the DSA as an opportunity to address implementation challenges and set a precedent for how such assessments can be conducted across jurisdictions.⁶⁹

The DSA's requirements mirror the UNGPs' call for companies to publicly communicate how they aim to exercise human rights due diligence in addressing the impact of their activities. Both frameworks emphasize responsible business conduct and require companies to identify, prevent, mitigate, and account for the impact on human rights through due diligence. The DSA specifically requires digital service providers to take measures to ensure that their services do not facilitate illegal activities or negative impacts on fundamental rights. Recital 79 of the DSA asserts that VLOP and VLOSE providers should assess the severity of the potential adverse impacts (scope, scale, and remediability as assessment criteria) as well as the probability of all such systemic risks when estimating the relevance of potential human rights infringements. For example, providers could consider if the potential harm will affect many people, where it will be irreversible, and how difficult it will be to remedy and restore the scenario that existed before the potential impact. It is important to note, however, that the DSA does not require companies to implement such measures prescribed in Recital 79, by only suggesting that companies "could" assess the criteria mentioned therein. The due diligence obligations of the DSA and

67 Sonia Livingstone et al., (2019). 'Is There a Ladder of Children's Online Participation? Findings from Three Global Kids Online Countries', Innocenti Research Brief 2019-02 (UNICEF, February 2019).

68 Frosio, G. (2022). Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering. *Regulating and Governing Private Ordering* (2022). (forthcoming in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law*, Edward Elgar), p. 17.

69 Allen, A. & Stockhem, O. (2022). A Series on the EU Digital Services Act: Due Diligence in Content Moderation. Center for Democracy and Technology. <https://cdt.org/insights/a-series-on-the-eu-digital-services-act-due-diligence-in-content-moderation/>.

the UNGP both aim to promote the protection of human rights in the digital age, with the DSA's obligations, on the one hand being specific to digital services, as well as being legally binding and enforceable, and the UNGPs, on the other hand, being broader in scope and applicable to all types of businesses and sectors.

Nonetheless, both frameworks reinforce the importance of responsible business practices that respect human rights. However, the DSA could more strongly emphasize the relevance of the UNGP's approach throughout, including the UNGP's calling for a prioritization when addressing adverse impacts based on the scope, scale and remediability of harm (saliency/severity), as well as the UNGP-based distinctions between risks that a company may cause, contribute to, or be directly linked to.⁷⁰ Foundational papers drafted by the OHCHR B-Tech Project, such as "Identifying and Assessing Human Rights Risks Related to End-Use"⁷¹ and "Taking Action to Address Human Rights Risks Related to End-Use"⁷² can be pivotal in better understanding how best to strengthen enforcement and implementation of business respect for human rights. Both these foundational papers aim at providing a common framework to align guidance and recommendations on ways that technology companies can adequately identify and address human rights risks stemming from their online services.

2.5. Access to Remedy

As previously mentioned (Section 1.1.), access to remedy is a core pillar of the UNGPs, and equally, a critical element of any regulatory framework aimed at promoting respect for human rights. Access to remedy entails that victims have access to effective judicial and State-based non-judicial grievance mechanisms and non-State-based grievance mechanisms; and that non-judicial grievance mechanisms must meet a set of effectiveness criteria (UNGP 31). While UNGP 26 addresses State-based judicial mechanisms, and UNGP 27 State-based non-judicial ones, UNGP 29 articulates that "business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted". Operational-level grievance mechanisms are meant to be accessible directly to individuals and communities who may have been or may be adversely impacted due to a business' actions. Their core aims are to i) support the business' ongoing human rights due diligence process by identifying adverse human rights impacts (i.e., through analysing trends

70 Key experts organizations agree on this point, such as the Global Network Initiative and the Digital Trust & Safety Partnership <https://globalnetworkinitiative.org/wp-content/uploads/2023/06/Discussion-summary---GNI-and-DTSP-workshops-on-implementing-risk-assessments-under-the-DSA-June-2023.pdf> p. 4.

71 OHCHR B-Tech Project. (2020). Identifying and Assessing Human Rights Risks Related to End-Use. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>.

72 OHCHR B-Tech Project. (2020). Taking Action to Address Human Rights Risks Related to End-Use. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/taking-action-address-human-rights-risks.pdf>.

and patterns in complaints), and ii) to address the harms identified and to remediate victims and preventing harms from expanding and grievances from rising. Such a measure provides victims a route to claim redressal without having to first access other means of recourse and can directly make claims against the business. As a means to increase accountability and enable remediation, UNGP 30 provides that collaborative initiatives, such as those established through framework agreements between trade unions and transnational corporations, are also expected to have effective mechanisms available where affected parties can raise their concerns. To reiterate, it is also the responsibility of businesses to provide for or cooperate in remediation of human rights harms they have caused/contributed to (UNGP 22).

Comparatively, the DSA includes provisions to ensure that those affected by online service providers have access to remedies. Due to the recent entering into force of the law, there are no precedent cases to be discussed yet. The DSA sets out that in cases of infringements, affected users and organisations mandated to exercise users' rights on their behalf have the right to seek collective redress. Interestingly, not only can individual claims against companies be made, but the DSA further foresees the possibility for collective redress under EU's Directive 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers.⁷³ The latter approach can be seen as consistent with UNGP 26, which speaks of the need to address barriers to effective judicial access. The DSA, in conjunction with EU's Directive 2020/1828, systematically provides avenues for affected users in collectively filing a case against a technology company, which could substantially improve people's right to redress as it relieves the high burden for them to seek redress individually.

A potential avenue for a company-led grievance mechanism may be found in Article 12 by which intermediary service providers are required to appoint a sole contact point that allows users to communicate with them directly and rapidly, using electronic methods in a user-friendly way. Information provided by users through the contact point can help identify potential human rights issues, such as hate speech or disinformation, and enable companies to take action to address them. By engaging with users in this way, companies can demonstrate their commitment to respecting user rights and promoting a safe and inclusive online environment. Though this provision itself does not provide clear guidance on what other methods should be made available to users, Recital 43 outlines that easily accessible means "such as telephone numbers, email addresses, electronic contact forms, chatbots, or instant messaging" should be made available. Article 12(1) further provides users of such services to be able to choose the means of communication, which does not only have to be automated ones. Online intermediary

73 Directive 2020/1828. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. <https://eur-lex.europa.eu/eli/dir/2020/1828/oj/eng>.

services should therefore make all reasonable efforts to ensure that sufficient human and financial resources are assigned to provide timely and efficient communication responses.

The DSA enables users to file complaints to the DSC, who will then determine which type of mechanism may best redress the harms caused, which may even be State-based non-judicial or non-State-based grievance mechanisms. These mechanisms include on the one hand **complaint handling systems**: Article 20 of the DSA states that online platform providers must offer recipients of the service access to an internal complaint-handling system for at least six months after a decision has been made. The system should allow for free and electronic complaint submissions against the platform's decision regarding notices of illegal content and other decisions made based on the recipients' provided information.

Another mechanism-like component is the **notice-and-action mechanisms** that enable users to report and request the removal of illegal or harmful content. Article 16 of the DSA requires that providers of hosting services to put in place mechanisms to notify any individual or entity of the presence of potentially illegal content. The possibility of **collective actions represented by "trusted flaggers"** (Article 22)⁷⁴ covers a way in which the Article 16 mechanism should function, such as consumer organizations or other qualified entities acting on behalf of individuals who have suffered harm because of the activities of VLOPs and VLOSEs. This could also entail non-users. This operational-level grievance mechanism can be an important tool for promoting access to remedy, particularly in cases where individual claims may be small or difficult to pursue through traditional legal channels. This mechanism also outsources some of the responsibility for content moderation from platforms to third parties, like with conventional "flaggers",⁷⁵ in other words users that report harmful content that they view online. However, with more authority, as they were given the "trusted" status by the DSC, these "flaggers" have been certified in their expertise and competence.⁷⁶ The certification diffuses the expectations towards company responsibility, making the practise both attractive and controversial. The mechanism is appealing to companies and users to a certain degree, as it provides a solution for platforms to compensate for lacking incentives, expertise, or legitimacy. However, it is also controversial as it can be used to serve the interest of certain groups, as not everyone trusts the same flaggers.⁷⁷

Such mechanisms can in many ways help companies mitigate specific instances of illegal content on online platforms through user complaints that can put companies on notice about specific

74 DSA, Article 22.

75 See: Crawford, K., & Gillespie, T. (2016). What is a flag for? Social media reporting tools and the vocabulary of complaint. *New Media & Society*, 18(3), 410-428.

76 DSA, Article 27(2).

77 Appelman, N., & Leerssen, P. (2022). On "Trusted" Flaggers. *Yale JL & Tech.*, 24, 452, p. 453-454.

instances.⁷⁸ It is, however, important to note that given the unprecedented number of content-related disputes that is to be expected under the DSA, affected users must be provided with adequate alternatives to traditional dispute settlement mechanisms.⁷⁹ One of them, provided by Article 21 DSA, calls for the participation of the DSCs. Beyond the DSCs' role in strengthening stakeholder participation, as mentioned in Section 2.2. of this study, the DSC of each Member State can additionally certify local dispute settlement bodies to offer services to all parties seeking redress against a platform decision.⁸⁰ Essentially, the DSA hopes to broaden the scope for dispute resolution by collaborating with different (private and public) dispute resolution bodies via this certification mechanism, as per Article 53 of the DSA.

Article 21 DSA also establishes a framework for **out-of-court dispute resolution** with regards to content moderation. Dispute resolution mechanisms include, for example, mediation or arbitration. They can be used to resolve disputes between online service providers and their users or business customers. These mechanisms are more flexible and efficient than traditional legal proceedings, which can be time-consuming, expensive, and complex. The parties involved may opt to seek resolution via a certified out-of-court dispute settlement body and parties may engage with said body in good faith. The certification process will be conducted by the DSA of the Member State in an impartial, independent, and expert manner, as in accordance with Article 18(3) of the DSA. However, following criticism to the initial proposal,⁸¹ the final draft of the DSA now states that the decision produced through such mechanisms are not binding on the parties, which raises the question of how effective a solution this will be.

However, it is worth noting that access to remedy under the DSA is still subject to certain limitations and challenges in the implementation phase, and a final appraisal from a UNGPs' perspective is difficult to make now. The policy debate on the effectiveness of the implementation of remedial mechanisms in the technology sector is not very advanced, and empirical evidence is limited, particularly in relation to the potential for complaint handling and notice-and-actions mechanisms to align with the criteria for non-judicial grievance mechanisms under the UNGPs. For example, the effectiveness of internal complaint-handling mechanisms may depend on the willingness of online service providers to engage in good faith and respond to complaints in a timely and appropriate manner. Similarly, alternative dispute resolution mechanisms may

78 Ortolani, P. (2023). If You Build it, They Will Come: The DSA "Procedure Before Substance" Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelmann, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. *Verfassungsbooks*. p. 156.

79 Ortolani, P. (2023). If You Build it, They Will Come: The DSA "Procedure Before Substance" Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelmann, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. *Verfassungsbooks*. p. 158.

80 Ortolani, P. (2023). If You Build it, They Will Come: The DSA "Procedure Before Substance" Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelmann, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. *Verfassungsbooks*. p. 159.

81 See: Wimmers, J. (2021). The out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 12, 381. And: Holznagel, D. (2022 March 16). A Self-Regulatory Race to the Bottom through Out-of-Court Dispute Settlement in the Digital Services Act: How the DSA will introduce competition for the Meta Oversight Board (and the German FSM) and why we should be worried about this. *Verfassungsblog*. <https://verfassungsblog.de/a-self-regulatory-race-to-the-bottom-through-art-18-digital-services-act/>.

not always be accessible or appropriate for all types of disputes, particularly those involving complex legal or technical issues. As regards non-State-based grievance mechanisms and operational-level grievance mechanisms, one of the most important indicators of their success is the extent to which they have sought and tailored the grievance mechanism to the needs, expectations, and perspectives of the people for whose use these mechanisms are intended. The grievance mechanisms need to be developed with the participation of rightsholders. The DSA overlooked this, though this could be addressed when implementing. Equally the rights of non-users adversely impacted by activities, e.g. happening on social media, such as incitement of violence, could be clarified.

As regards State-based non-judicial mechanisms, there is a need for mechanisms to be developed with a clear idea of how they fit into the wider regulatory architecture, and how they will interact with existing mechanisms / systems. The Accountability and Remedy Project at UN Human Rights provides guidance on how individual mechanisms can meet the effectiveness criteria.⁸² Furthermore, the B-Tech Project provides for additional guidance on enabling an “Access to Remedy Ecosystem Approach”,⁸³ which recommends ways that technology companies and governments can work together to address gaps in coverage of different mechanisms and to promote greater coherence and inter-operability of different regimes and processes. Another foundational paper drafted by the B-Tech Project, “Designing and Implementing Effective Company-Based Grievance Mechanisms”,⁸⁴ alludes to the ways technology companies can navigate through best practices and enforce measures that are most effective in remediating users. In terms of the DSA having stronger alignment with the UNGPs, the next section 3.4. will provide guidance recommendations on ways in which the EC can strengthen the enforcement of, and companies can improve the compliance with the DSA.

3. RECOMMENDATIONS

The current state of the implementation debate around the DSA is critical.⁸⁵ Stakeholders have praised early involvement of civil society in the drafting process, while strong corporate lobbying has been criticized in a range of media outlets.⁸⁶ Many enforcement provisions are subject to

82 OHCHR Accountability and Remedy Project: <https://www.ohchr.org/en/business/ohchr-accountability-and-remedy-project/phase2-state-based-non-judicial-mechanisms>.

83 OHCHR B-Tech Project. (2021). Access to Remedy Ecosystem Approach. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-ecosystem-approach.pdf>.

84 OHCHR B-Tech Project. (2021). Designing and Implementing Effective Company-Based Grievance Mechanisms. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-company-based-grievance-mechanisms.pdf>.

85 Ortolani, P. (2023). If You Build it, They Will Come: The DSA “Procedure Before Substance” Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelmann, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. *Verfassungsbooks*.

86 Article 19. (2019). Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence. https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

the Delegated Acts. The designation of Digital Services Coordinators who will be responsible for enforcement at the Member State level is due to conclude in early 2024.

The inclusion of fundamental rights in the new wave of EU digital regulation, such as the DSA, represents significant regulatory progress. The DSA regulation aims to establish a more comprehensive and fitting framework for safeguarding individuals. This is particularly important in an era marked by pervasive technologies that are often developed without adequate consideration of their societal impact.⁸⁷ Conversations with human rights experts working in companies subject to the DSA suggest some concern that the legislation may take away agency from the human rights teams in favour of adopting a compliance-focused approach. They recommend specifying the human rights terminology, particularly on human rights due diligence.⁸⁸

The implementation and enforcement of the DSA will require careful consideration of several key questions. The following key recommendations, which play homage to the UNGPs, will be important to guide the next steps for the DSA implementation and enforcement:

Stakeholder engagement requirements

- Emphasise that complying with the DSA needs to include robust stakeholder engagement. This should include demanding companies to identify key stakeholders to their operations, where priority should be given to potentially adversely affected groups, including non-users.
- At the same time, recognize and provide support to mechanisms that will help address stakeholder fatigue and ensure that engagement is conducted appropriately in ways that recognize the value provided by stakeholders and that encourage meaningful feedback loops.
- Seek to achieve policy coherence in relation to other ongoing legislative processes at the EU level, such as the Corporate Sustainability Due Diligence Directive.
- Provide for a strong role of civil society in monitoring the implementation of the DSA and holding platforms and enforcement bodies to account. This could be done by making sure that civil society is structurally integrated into follow-up mechanisms, such as in the drafting of forthcoming guidance, or consulted through a formal mechanism of exchange with enforcement bodies at national and EU level.

87 Mantelero, A. (2022). Fundamental rights impact assessments in the DSA. Verfassungsblog: On Matters Constitutional. https://intr2dok.vifa-recht.de/receive/mir_mods_00014449.

88 OHCHR B-Tech & CDT Europe. (2023). Fostering Responsible Business Conduct in the Tech Sector – the Need for Aligning Risk Assessment, Transparency and Stakeholder Engagement Provisions under the EU Digital Services Act with the UNGPs. https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/B-Tech_Blog_RBC_DSA_UNGPs-alignment.pdf

Transparency

- Ensure disclosures by companies are structured in a format that allows for meaningful information to be accessible by stakeholders, including about how voices from potentially affected stakeholder groups, including users and non-users, have contributed to company policy. The format as such should be easily readable, without contributing to over-information fatigue.
- Require companies to make information public by using clearly defined metrics and methodologies to allow stakeholders to differentiate laggards from responsible leaders, and track progress over time about content moderation policies, procedures, and practices and how these relate to human rights.
- Support a framework for research access to data that is open to qualified and credible civil society and academic researchers, including those outside of Europe who are studying the cross-border impacts of platforms and platform regulations. Coordinate with other regulators in other democratic countries, who will be establishing similar frameworks, to ensure efficiency and effectiveness in these approaches.
- Align follow-up mechanisms with the UNGPs, including the enforcement architecture, including for transparency requirements. The recommendations and guidance produced by the UN B-Tech Project and [Accountability and Remedy Project](#) of OHCHR should contribute to the design of the enforcement architecture. These documents include guidance on how to enhance effectiveness of State and non-State-based judicial and non-judicial grievance mechanisms.

Risk assessment methodologies

- Often communicated as an “adaptive regulation”, the DSA provides for several follow-up mechanisms. Such mechanisms should enable further clarity as to how “systemic risk” related to the dissemination of content relates to the international human rights framework.⁸⁹ The mechanisms should also ensure alignment with the UNGPs is upheld and accordingly implemented in business practices. The B-Tech Project has published helpful guidance in this regard.⁹⁰
- Ensure alignment of EU DSA delegated Acts and Guidelines with international human rights standards, particularly with the UNGPs, and align the terminology around the interpretation of “systemic risks” accordingly.

89 Key experts organizations raise similar points, such as the Global Network Initiative and the Digital Trust & Safety Partnership <https://globalnetworkinitiative.org/wp-content/uploads/2023/06/Discussion-summary---GNI-and-DTSP-workshops-on-implementing-risk-assessments-under-the-DSA-June-2023.pdf> p. 3.

90 OHCHR B-Tech. (2020). Identifying and Assessing Human Rights Risks related to End-Use. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>.

- Seek to achieve policy coherence in relation to other ongoing legislative processes at the EU level, such as the Corporate Sustainability Due Diligence Directive.
- Support mechanisms and create spaces that allow civil society, platforms, and auditors to candidly discuss challenges and exchange lessons learned regarding risk assessment and mitigation.
- Clarify the expectations towards human rights risk assessment and the importance of assessing human rights risks stemming from or being linked to platform activities requiring prioritization of measures according to the severity of potential adverse impacts (scope, scale, and remediability as assessment criteria); this includes specifying what constitutes a good risk assessment regarding risk to people for the purpose of auditing.

Access to Remedy

- Align grievance mechanisms with the UNGPs effectiveness criteria⁹¹, in particular in relation to complaint handling systems/any type of operational-level grievance mechanisms operated by companies.
- Ensure access to remedy for non-users who may be adversely impacted.
- Ensure Transparency and clarity about the way that decisions are taken, and the circumstances in which decisions may be challenged and reviewed.⁹²
- Provide a form of independent review of decision-making to enhance the credibility of mechanisms with affected people and groups.⁹³
- Strengthen rules on the conduct of trusted flaggers and ensure that severity is at the forefront when content is flagged as harmful. Additionally, clear rules should be set in place to ensure that the trusted flaggers are not endowed with excess power, which may lead to over-enforcement and disproportionality.
- Ensure that State-based grievance mechanisms and operational-level grievance mechanisms are tailored to the needs, expectations, and perspectives of the people for whose use these mechanisms are intended. The mechanisms need to be developed with the participation of rightsholders.
- Foster non-judicial grievance mechanisms to be developed with a clear idea of how they fit into the wider regulatory architecture, and how they will interact with existing mechanisms / systems.

91 OHCHR. (2021). OHCHR Accountability and Remedy Project: Meeting the UNGPs' Effectiveness Criteria. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2022-01/arp-note-meeting-effectiveness-criteria.pdf>.

92 OHCHR B-Tech. (2021). Access to Remedy and the Technology Sector: Understanding the Perspectives and Needs of Affected People and Groups. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/B-Tech/access-to-remedy-perspectives-needs-affected-people.pdf>.

93 *ibid.*

REFERENCES

Allen, A. & Stockhem, O. (2022 August 10). A Series on the EU Digital Services Act: Due Diligence in Content Moderation. Center for Democracy and Technology. <https://cdt.org/insights/a-series-on-the-eu-digital-services-act-due-diligence-in-content-moderation/>.

Appelman, N., & Leerssen, P. (2022). On "Trusted" Flaggers. *Yale JL & Tech.*, 24, 452. p. 453–454.

Article 19. (2019). Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence. https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

Article 19. (2020 April 7). EU: Terrorist Content Regulation must protect freedom of expression rights. <https://www.article19.org/resources/eu-terrorist-content-regulation-must-protect-freedom-of-expression-rights/>; And: La Quadrature du Net (LQDN). (2022 March 9). French deputies must reject online censorship without a judge in one hour. <https://edri.org/our-work/french-deputies-must-reject-online-censorship-without-a-judge-in-one-hour/>; And: Rojszczak, M. (2022). Online content filtering in EU law—A coherent framework or jigsaw puzzle?. *Computer Law & Security Review*, 47, 105739.

Bedi, I. (2023 February 20). The Territorial Scope of the EU Digital Services Act: Isaac Bedi considers the territorial scope of the EU Digital Services Act and how it will apply to organisations outside of the EU. *Burges-Salmon*. <https://www.burges-salmon.com/news-and-insight/legal-updates/technology-and-communications/the-territorial-scope-of-the-eu-digital-services-act#:~:text=What%20is%20the%20territorial%20scope.in%20a%20world%20without%20borders>.

Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12(4), 758–774. doi:10.1017/err.2021.8. p. 772.

Chini, M. (2022 April 23). 'What is illegal offline is illegal online': EU tightens rules for internet giants. *The Brussels Times*. <https://www.brusselstimes.com/219152/what-is-illegal-offline-is-illegal-online-eu-tightens-rules-for-internet-giants>.

Clifford Chance. (2022). The digital services act: what is it and what impact will it have?. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/the-digital-services-act-what-is-it-and-what-impact-will-it-have-updated-december-2022.pdf>, p. 4.

Crawford, K., & Gillespie, T. (2016). What is a flag for? Social media reporting tools and the vocabulary of complaint. *New Media & Society*, 18(3), 410–428.

De Schutter, O. (2013). Foreword: Beyond the Guiding Principles. In: Deva, S. & Bilchitz, D. (eds.) *Human rights obligations of business: Beyond the corporate responsibility to respect?* Cambridge University Press, Cam-

bridge, pp. xv–xxii.

Dietrich, M., Jung, N., and van Rooijen, A. (2022 November 25). Digital Regulation in Europe. Global Competition Review. Digital Markets Guide – Second Edition. Global Competition Review. <https://globalcompetitionreview.com/guide/digital-markets-guide/second-edition/article/digital-regulation-in-europe>.

Directive 2020/1828. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. <https://eur-lex.europa.eu/eli/dir/2020/1828/oj/eng>.

Ebert, I., & Beduschi, A. (2022). Regulating business conduct in the technology sector: Gaps and Ways Forward in applying the UNGPs. <https://ore.exeter.ac.uk/repository/bitstream/handle/10871/129465/Regulating%20business%20conduct%20in%20the.pdf?sequence=1>. p. 3.

European Broadcasting Union (EBU). (2023). Digital Services Act: A Handbook For Public Service Media. EBU Legal and Policy. <https://www.ebu.ch/files/live/sites/ebu/files/Publications/Reports/open/10022023-Digital-Services-Act-Handbook%E2%80%93Public-Version.pdf>, p. 4.

European Commission. (2022 November 16). Digital Services Act: EU’s landmark rules for online platforms enter into force. EC Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906.

European Commission. (2023 April 25). Questions and Answers – Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.

European Commission. (2023). Shaping Europe’s digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

European Commission. (2023). Shaping Europe’s digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

Frosio, G. (2022). Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering. Regulating and Governing Private Ordering (October 3, 2022). (forthcoming in Andrej Savin and Jan Trzaskowski (eds), Research Handbook on EU Internet Law, Edward Elgar).

Holly, G. et. al. (2023). How do the pieces fit in the puzzle? Making sense of EU regulatory initiatives related to business and human rights. The Danish Institute for Human Rights. https://www.humanrights.dk/files/media/document/2023_06_02_EU-RegulatoryMeasuresExplainer_EN_june2023.pdf.

ICCL. (2023). 5 years: GDPR’s crisis point ICCL report on EEA data protection authorities. <https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf>.

Ingrams, M. G. & Wilde–Ramsing, J. (2023 12 June). Updated OECD Guidelines reconfirm downstream application of due diligence. Cambridge Core Blog. <https://www.cambridge.org/core/blog/2023/06/12/updated-oecd-guidelines-reconfirm-downstream-application-of-due-diligence/>.

Mantelero, A. (2022). Fundamental rights impact assessments in the DSA. Verfassungsblog: On Matters Constitutional. https://intr2dok.vifa-recht.de/receive/mir_mods_00014449.

Minović, A. (2022 August 7). GDPR: Integrating human rights into business practices. DIPLO. <https://www>.

diplomacy.edu/blog/gdpr-integrating-human-rights-business-practices/.

OECD. (2018). Due Diligence Guidance for Responsible Business Conduct. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>.

OECD. (2023). OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. <https://doi.org/10.1787/81f92357-en>.

OHCHR B-Tech Project. (2019). B-Tech Project OHCHR and business and human rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/en/business-and-human-rights/b-tech-project>.

OHCHR B-Tech Project. (2021). Access to Remedy: Concept and Principles. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>.

OHCHR B-Tech Project. 2020. The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>.

OHCHR B-Tech. (2020). Identifying and Assessing Human Rights Risks related to End-Use. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>.

OHCHR B-Tech. (2020). Key Characteristics of Business Respect for Human Rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/key-characteristics-business-respect.pdf>.

OHCHR B-Tech. (2021). Access to remedy and the technology sector: understanding the perspectives and needs of affected people and groups. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-perspectives-needs-affected-people.pdf>.

OHCHR B-Tech. (2021). The Strategic Aspects of Business Respect for Human Rights Part One: Overview and Reflections on Current Practice. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2021-11/strategic-aspects-part-1.pdf>.

OHCHR B-Tech. (2022). The Feasibility of Mandating Downstream Human Rights Due Diligence: Reflections from technology company practices. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/documents/issues/business/2022-09-13/tech-downstream-hrdd.pdf>.

OHCHR B-Tech & CDT Europe. (2023). Fostering Responsible Business Conduct in the Tech Sector – the Need for Aligning Risk Assessment, Transparency and Stakeholder Engagement Provisions under the EU Digital Services Act with the UNGPs. <https://www.ohchr.org/sites/default/files/documents/issues/business/b->

[tech/B-Tech_Blog_RBC_DSA_UNGPs-alignment.pdf](https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf).

OHCHR. (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. (HR/PUB/11/04). United Nations. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

OHCHR. (2021). OHCHR Accountability and Remedy Project: Meeting the UNGPs’ Effectiveness Criteria. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2022-01/arp-note-meeting-effectiveness-criteria.pdf>.

OHCHR. (n.d.). The UN Guiding Principles On Business And Human Rights An Introduction. The UN Working Group On Business And Human Rights. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf.

Ortolani, P. (2023). If You Build it, They Will Come: The DSA “Procedure Before Substance” Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelmann, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. Verfassungsbooks.

Pelkmans, J., & Renda, A. (2014). How can EU legislation enable and/or disable innovation. European Commission.

Pop, F. (2022, September 6). The Digital Services Act: Creating accountability for online platforms and protecting users’ rights? EIPA. <https://www.eipa.eu/blog/the-digital-services-act-creating-accountability-for-online-platforms-and-protecting-users-rights/>.

Regulation 2022/2065. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). <http://data.europa.eu/eli/reg/2022/2065/oj>.

Rojszczak, M. (2022). Online content filtering in EU law—A coherent framework or jigsaw puzzle?. *Computer Law & Security Review*, 47, 105739.

Ruggie, J. (2011). Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises. (A/HRC/17/31). Human Rights Council. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf. p. 244.

Sherman, J. (2020). Beyond CSR: The Story of the UN Guiding Principles on Business and Human Rights. Corporate Responsibility Initiative. Harvard Kennedy School. Working Paper No. 71. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/CRI_AWP_71.pdf.

Singh, S. (2022 January 21). The EU’s Digital Services Act Makes a Positive Step Towards Transparency and Accountability, But Also Raises Some Serious Questions. *New America*. <https://www.newamerica.org/oti/blog/the-eus-digital-services-act-makes-a-positive-step-towards-transparency-and-accountability-but-also-raises-some-serious-questions/>.

Sonia Livingstone et al., ‘Is There a Ladder of Children’s Online Participation? Findings from Three Global

Kids Online Countries', Innocenti Research Brief 2019-02 (UNICEF, February 2019). Livingstone, Sonia, Daniel Kardefelt-Winther, Petar Kanchev, Patricio Cabello, Magdalena Claro, Patrick Burton, and Joanne Phyfer. 'Is There a Ladder of Children's Online Participation? Findings from Three Global Kids Online Countries'. Innocenti Research Brief 2019-02. UNICEF, February 2019.

Van den Brande, B. (2022 November 7). The Digital Services Act has been approved: targeted advertising will soon be restricted. Lexology. <https://www.lexology.com/library/detail.aspx?g=cefceeff-6426-4c2c-8cec-b45cae3381b8>.

Wimmers, J. (2021). The out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 12, 381. And: Holzengel, D. (2022 March 16). A Self-Regulatory Race to the Bottom through Out-of-Court Dispute Settlement in the Digital Services Act: How the DSA will introduce competition for the Meta Oversight Board (and the German FSM) and why we should be worried about this. *Verfassungsblog*. <https://verfassungsblog.de/a-self-regulatory-race-to-the-bottom-through-art-18-digital-services-act/>.

Wolfsteller, R., Li, Y. Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness. *Hum Rights Rev* 23, 1-17 (2022). #References

Allen, A. & Stockhem, O. (2022 August 10). A Series on the EU Digital Services Act: Due Diligence in Content Moderation. Center for Democracy and Technology. <https://cdt.org/insights/a-series-on-the-eu-digital-services-act-due-diligence-in-content-moderation/>.

Appelman, N., & Leerssen, P. (2022). On "Trusted" Flaggers. *Yale JL & Tech.*, 24, 452. p. 453-454.

Article 19. (2019). Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence. https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

Article 19. (2020 April 7). EU: Terrorist Content Regulation must protect freedom of expression rights. <https://www.article19.org/resources/eu-terrorist-content-regulation-must-protect-freedom-of-expression-rights/>; And: La Quadrature du Net (LQDN). (2022 March 9). French deputies must reject online censorship without a judge in one hour. <https://edri.org/our-work/french-deputies-must-reject-online-censorship-without-a-judge-in-one-hour/>; And: Rojszczak, M. (2022). Online content filtering in EU law—A coherent framework or jigsaw puzzle?. *Computer Law & Security Review*, 47, 105739.

Bedi, I. (2023 February 20). The Territorial Scope of the EU Digital Services Act: Isaac Bedi considers the territorial scope of the EU Digital Services Act and how it will apply to organisations outside of the EU. Burges-Salmon. [https://www.burges-salmon.com/news-and-insight/legal-updates/technology-and-communications/the-territorial-scope-of-the-eu-digital-services-](https://www.burges-salmon.com/news-and-insight/legal-updates/technology-and-communications/the-territorial-scope-of-the-eu-digital-services-act)

[act#:~:text=What%20is%20the%20territorial%20scope,in%20a%20world%20without%20borders.](#)

Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12(4), 758-774. doi:10.1017/err.2021.8. p. 772.

Chini, M. (2022 April 23). 'What is illegal offline is illegal online': EU tightens rules for internet giants. *The Brussels Times*. <https://www.brusselstimes.com/219152/what-is-illegal-offline-is-illegal-online-eu-tightens-rules-for-internet-giants>.

Clifford Chance. (2022). The digital services act: what is it and what impact will it have?. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/the-digital-services-act-what-is-it-and-what-impact-will-it-have-updated-december-2022.pdf>, p. 4.

Crawford, K., & Gillespie, T. (2016). What is a flag for? Social media reporting tools and the vocabulary of complaint. *New Media & Society*, 18(3), 410-428.

De Schutter, O. (2013). Foreword: Beyond the Guiding Principles. In: Deva, S. & Bilchitz, D. (eds.) *Human rights obligations of business: Beyond the corporate responsibility to respect?* Cambridge University Press, Cambridge, pp. xv-xxii.

Dietrich, M., Jung, N., and van Rooijen, A. (2022 November 25). Digital Regulation in Europe. *Global Competition Review. Digital Markets Guide – Second Edition*. Global Competition Review. <https://globalcompetitionreview.com/guide/digital-markets-guide/second-edition/article/digital-regulation-in-europe>.

Directive 2020/1828. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. <https://eur-lex.europa.eu/eli/dir/2020/1828/>

[oj/eng](https://eur-lex.europa.eu/eli/dir/2020/1828/oj/eng). consumers and repealing Directive 2009/22/EC. <https://eur-lex.europa.eu/eli/dir/2020/1828/oj/eng>.

Ebert, I., & Beduschi, A. (2022). Regulating business conduct in the technology sector: Gaps and Ways Forward in applying the UNGPs. <https://ore.exeter.ac.uk/repository/bitstream/handle/10871/129465/Regulating%20business%20conduct%20in%20the.pdf?sequence=1>. p. 3.

European Broadcasting Union (EBU). (2023). Digital Services Act: A Handbook For Public Service Media. EBU Legal and Policy. <https://www.ebu.ch/files/live/sites/ebu/files/Publications/Reports/open/10022023-Digital-Services-Act-Handbook%E2%80%93Public-Version.pdf>, p. 4.

European Commission. (2022 November 16). Digital Services Act: EU's landmark rules for online platforms enter into force. EC Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906.

European Commission. (2023 April 25). Questions and Answers – Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.

European Commission. (2023). Shaping Europe's digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

European Commission. (2023). Shaping Europe's digital future: The Digital Services Act Package. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

Frosio, G. (2022). Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering. Regulating and Governing Private Ordering (October 3, 2022). (forthcoming in Andrej Savin and Jan Trzaskowski (eds), Research Handbook on EU Internet Law, Edward Elgar). www.humanrights.dk/files/media/document/2023_06_02_EU-RegulatoryMeasuresExplainer_EN_june2023.pdf.

ICCL. (2023). 5 years: GDPR's crisis point ICCL report on EEA data protection authorities. <https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf>.

Ingrams, M. G. & Wilde-Ramsing, J. (2023 12 June). Updated OECD Guidelines reconfirm downstream application of due diligence. Cambridge Core Blog. <https://www.cambridge.org/core/blog/2023/06/12/updated-oecd-guidelines-reconfirm-downstream-application-of-due-diligence/>.

Mantelero, A. (2022). Fundamental rights impact assessments in the DSA. Verfassungsblog: On Matters Constitutional. https://intr2dok.vifa-recht.de/receive/mir_mods_00014449.

Minović, A. (2022 August 7). GDPR: Integrating human rights into business practices. DIPLO. <https://www.diplomacy.edu/blog/gdpr-integrating-human-rights-business-practices/>.

OECD. (2018). Due Diligence Guidance for Responsible Business Conduct. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>.

- OECD. (2023). OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. <https://doi.org/10.1787/81f92357-en>.
- OHCHR B-Tech Project. (2019). B-Tech Project OHCHR and business and human rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/en/business-and-human-rights/b-tech-project>.
- OHCHR B-Tech Project. (2021). Access to Remedy: Concept and Principles. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>.
- OHCHR B-Tech Project. 2020. The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>.
- OHCHR B-Tech. (2020). Identifying and Assessing Human Rights Risks related to End-Use. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>.
- OHCHR B-Tech. (2020). Key Characteristics of Business Respect for Human Rights. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/key-characteristics-business-respect.pdf>.
- OHCHR B-Tech. (2021). Access to remedy and the technology sector: understanding the perspectives and needs of affected people and groups. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-perspectives-needs-affected-people.pdf>.
- OHCHR B-Tech. (2021). The Strategic Aspects of Business Respect for Human Rights Part One: Overview and Reflections on Current Practice. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2021-11/strategic-aspects-part-1.pdf>.
- OHCHR B-Tech. (2022). The Feasibility of Mandating Downstream Human Rights Due Diligence: Reflections from technology company practices. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/documents/issues/business/2022-09-13/tech-downstream-hrdd.pdf>.
- OHCHR B-Tech & CDT Europe. (2023). Fostering Responsible Business Conduct in the Tech Sector – the Need for Aligning Risk Assessment, Transparency and Stakeholder Engagement Provisions under the EU Digital Services Act with the UNGPs. https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/B-Tech_Blog_RBC_DSA_UNGPs-alignment.pdf.
- OHCHR. (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. (HR/PUB/11/04). United Nations. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

- OHCHR. (2021). OHCHR Accountability and Remedy Project: Meeting the UNGPs' Effectiveness Criteria. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/sites/default/files/2022-01/arp-note-meeting-effectiveness-criteria.pdf>.
- OHCHR. (n.d.). The UN Guiding Principles On Business And Human Rights An Introduction. The UN Working Group On Business And Human Rights. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf.
- Ortolani, P. (2023). If You Build it, They Will Come: The DSA "Procedure Before Substance" Approach. In: Hoboken, J., Buri, I., Quintais, J., Fahy, R., Appelman, N., & Straub, M. (2023). Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications. Verfassungsbooks.
- Pelkmans, J., & Renda, A. (2014). How can EU legislation enable and/or disable innovation. European Commission.
- Pop, F. (2022, September 6). The Digital Services Act: Creating accountability for online platforms and protecting users' rights? EIPA. <https://www.eipa.eu/blog/the-digital-services-act-creating-accountability-for-online-platforms-and-protecting-users-rights/>.
- Regulation 2022/2065. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). <http://data.europa.eu/eli/reg/2022/2065/oj>.
- Rojszczak, M. (2022). Online content filtering in EU law—A coherent framework or jigsaw puzzle?. *Computer Law & Security Review*, 47, 105739.
- Ruggie, J. (2011). Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises. (A/HRC/17/31). Human Rights Council. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf. p. 244.
- Sherman, J. (2020). Beyond CSR: The Story of the UN Guiding Principles on Business and Human Rights. Corporate Responsibility Initiative. Harvard Kennedy School. Working Paper No. 71. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/CRI_AWP_71.pdf.
- Singh, S. (2022 January 21). The EU's Digital Services Act Makes a Positive Step Towards Transparency and Accountability, But Also Raises Some Serious Questions. *New America*. <https://www.newamerica.org/oti/blog/the-eus-digital-services-act-makes-a-positive-step-towards-transparency-and-accountability-but-also-raises-some-serious-questions/>.
- Sonia Livingstone et al., 'Is There a Ladder of Children's Online Participation? Findings from Three Global Kids Online Countries', Innocenti Research Brief 2019-02 (UNICEF, February 2019). Livingstone, Sonia, Daniel Kardefelt-Winther, Petar Kanchev, Patricio Cabello, Magdalena Claro, Patrick Burton, and Joanne Phyfer. 'Is There a Ladder of Children's Online Participation? Findings from Three Global Kids Online Countries'. Innocenti Research Brief 2019-02. UNICEF, February 2019.

Van den Brande, B. (2022 November 7). The Digital Services Act has been approved: targeted advertising will soon be restricted. Lexology. <https://www.lexology.com/library/detail.aspx?g=cefceeff-6426-4c2c-8cec-b45cae3381b8>.

Wimmers, J. (2021). The out-of-Court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 12, 381. And: Holznagel, D. (2022 March 16). A Self-Regulatory Race to the Bottom through Out-of-Court Dispute Settlement in the Digital Services Act: How the DSA will introduce competition for the Meta Oversight Board (and the German FSM) and why we should be worried about this. *Verfassungsblog*. <https://verfassungsblog.de/a-self-regulatory-race-to-the-bottom-through-art-18-digital-services-act/>.

Wolfsteller, R., Li, Y. Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness. *Hum Rights Rev* 23, 1-17 (2022).