Part III
Rights

Digitalisation and International Human Rights Law: Opportunities and Critical Challenges

Stefanie Schmahl

Abstract At the time when the various universal and regional human rights treaties came into being, the digitalization of societies was still largely in its infancy. Only a very few human rights treaties dealt with the influence of the media and the Internet on situations relevant to the protection of human rights. Nowadays, the parameters have changed fundamentally. Numerous UN human rights committees are increasingly confronted with questions of digitalization and its effects on the legal position of the individual. The same applies to international courts at the regional level, in particular to the European Court of Human Rights. However, their decisions still focus mainly on substantive human rights issues, for instance, by resorting to an evolutive interpretation to outline the freedom of communication and the right to private life in the digital environment. The overall effects of the Internet and the growing digitalization of societies on the general dogmatic aspects of human rights treaties have not yet been thoroughly investigated. The aim of the chapter is, therefore, to shed a first light on the main challenges that typically arise when determining the structural relationship between international human rights norms on the one hand and behaviours of individuals in the digital environment on the other. These challenges relate to specific structural features such as the existence or non-existence of a right to access the Internet, the contouring of new digital spheres of human rights and the dangers resulting from the use of algorithms and increasing anonymization. It is also questionable whether the scope of the extraterritorial application of human rights treaties needs to be redesigned in the digital age. Finally, more general human rights aspects such as the determination and possible extension of both duty-bearers and rights-holders require closer analysis. The chapter examines to what extent a dynamic interpretation of human rights treaties appears possible in the age of digitalization and under what conditions this approach reaches its limits.

I. Introduction

At the time when the various universal and regional human rights treaties came into being, the digitalisation of societies was still largely in its infancy. The 1989 Convention on the Rights of the Child (CRC)[1] was the first, and so far, is the only international human rights convention that explicitly addresses a question touching upon digitisation, namely the influence of the (digital) media on situations relevant to the protection of human rights. From the initial draft proposal to include a protective regulatory clause against potential negative effects of media on children in the

1 Convention on the Rights of the Child of 20 November 1989, 1577 UNTS 3.

Convention[2] arose finally an extensive and rich text, which also recognises and promotes the positive opportunities that the mass media have on the evolvement and education of children.[3] In view of its elaboration in the 1980s, it is, however, obvious that 'media' within the meaning of Article 17 CRC were mainly understood to include those of the analogue world, such as books, magazines, radio and cinema films.[4]

In order to sound out the scope of Article 17 CRC in the digital age, at the initiative of the CRC Committee, numerous representatives of States, international organisations and non-governmental organisations held a joint 'Day of General Discussion' in 2014 on the media behaviour of children in general. Another 'Day of General Discussion' in the same year dealt specifically with the use of digital media by children. The results of both discussion days are reflected in two legally non-binding recommendations of the CRC Committee.[5] Both documents stress and further specify the importance of Article 17 CRC and its close relationship with other Convention guarantees, such as the right to private life, freedom of expression and information, and the protection of children against economic and sexual exploitation.[6] The CRC Committee repeatedly emphasises that the content of those guarantees does not only refer to selected types of media. Rather, the scope of the standard extends equally to analogue and digital media by way of a dynamic interpretation.[7] Thus, it is not astonishing

2 See UN Commission on Human Rights, Revised Draft Convention on the Rights of the Child of 30 July 1980, E/CN.4/1349, p. 4.

3 For more detail see Sharon Detrick, *A Commentary on the United Nations Convention on the Rights of the Child* (Leiden: Martinus Nijhoff 1999), 285–287.

4 See Kai Hanke, Luise Meergans and Isabell Rausch-Jarolimek, 'Kinderrechte im Medienzeitalter. Ausführungen zum Recht des Kindes auf Medienzugang gemäß Art. 17 UN-Kinderrechtskonvention,' RdJB 65 (2017), 330–350 (335).

5 CRC Committee, 'Day of General Discussion on the child and the media,' 12 September 2014, CRC/C/15/Add.65, and 'Day of General Discussion on digital media and children's rights,' 12 September 2014.

6 For more detail see Stefanie Schmahl, 'Kinderrechte und Medien – Herausforderungen eines modernen Risiko- und Befähigungsmanagements' in: Ingo Richter, Lothar Krappmann and Friederike Wapler (eds), *Kinderrechte. Handbuch des deutschen und internationalen Kinder- und Jugendrechts* (Baden-Baden: Nomos 2020), 375–403 (378–380).

7 See, e.g., CRC Committee, 'Day of General Discussion on the child and the media,' 12 September 2014, CRC/C/15/Add.65, para. 256, point 5 and 'General Comment No. 16,' 17 April 2013, CRC/C/GC/16, para. 60. For more detail see John Tobin and Elizabeth Handsley, 'Article 17' in: John Tobin (ed.), *The UN Convention on the Rights of the Child. A Commentary* (Oxford: Oxford University Press 2019), 600 (605–606).

that the CRC Committee recently, on 2 March 2021, released a new General Comment No. 25 on children's rights in relation to the digital environment and gives guidance on how to respect, protect and fulfil children's rights in the digital environment.[8] Even if General Comment No. 25 merely summarises the Committee's previous considerations on the matter, it is the first General Comment of a UN human rights treaty body that explicitly addresses the digital environment and its impacts on human rights by highlighting both the empowering character and the risks of the digital environment for children's rights. In that regard, the CRC Committee functions as a human rights seismograph, being the first UN human rights treaty body to deal with rising fundamental questions in modern human rights law.[9]

In addition to the CRC Committee, also other treaty-based expert committees and human rights courts are increasingly confronted with questions of digitalisation and its effects on the legal position of the individual. The UN human rights monitoring bodies unanimously underscore that the Internet and social media can be valuable tools for providing information and opportunities for debate.[10] In particular, it is undisputed that the right to freedom of expression and information clearly extends to cyberspace. As early as 2012, the UN Human Rights Council stated that 'the same rights that people have offline must also be protected online, in particular, freedom of expression, which is applicable regardless of frontiers and through any media of one's choice.'[11] This statement has been endorsed by the UN Human Rights Committee in several instances.[12] On the regional level, the African Commission on Human and Peoples'

8 CRC Committee, 'General Comment No. 25,' 2 March 2021, CRC/C/GC/25, paras 22 ff.

9 See Stephan Gerbig, 'Leaving the Pre-Digital Era, Finally!: Thoughts on the New UN CRC General Comment on Children's Rights in the Digital Environment,' Völkerrechtsblog, 4 May 2021, DOI: 10.17176/20210504–111252–0.

10 See, e.g., Human Rights Committee, 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, para. 12; CESCR Committee, 'General Comment No. 25,' 30 April 2020, E/C.12/GC/25, paras 42, 45; CEDAW Committee/CRC Committee, 'Joint General Recommendation No. 31/General Comment No. 18,' 14 November 2014, CEDAW/C/GC/31-CRC/C/GC/18, para. 79.

11 Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet,' 16 July of 2012, HRC/RES/20/8, para. 1.

12 See, e.g., Human Rights Committee, 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, paras 12 ff. and 'General Comment No. 37,' 27 July 2020, CCPR/C/GC/37, para. 34.

Rights (ACHPR),[13] the Inter-American Commission of Human Rights (IACHR) and, the Inter-American Court of Human Rights (IACtHR)[14] as well as the European Court of Human Rights (ECtHR)[15] have also made it clear that freedom of expression and information applies to Internet communication.

Furthermore, almost all human rights conventions guarantee the right to a private life, which generally includes the integrity of personal data.[16] The UN Human Rights Council,[17] the UN Special Rapporteurs on freedom of expression and the right to privacy,[18] the UN General Assembly,[19] the Office of the High Commissioner for Human Rights (OHCHR),[20] the UN Human Rights Committee,[21] the European Union Agency for Fundamental Rights (FRA),[22] the Court of Justice of the European Union

13 See ACHPR, 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa, 4 November 2016, ACHPR/Res. 362(LIX)' and 'Declaration of Principles on Freedom of Expression and Access to Information in Africa,' 10 November 2019, Principle 17.

14 See IACHR, 'Standards for a Free, Open, and Inclusive Internet,' 15 March 2017, OEA/Ser.L/V/II and CIDH/RELE/INF.17/17; IACtHR, *Herrera-Ulloa v. Costa Rica*, judgment of 2 July 2004, paras 108 ff.

15 See, e.g., ECtHR, *MTE v. Hungary*, judgment of 2 February 2016, no. 22947/13, para. 56 and *Kharitonov v. Russia*, judgment of 23 June 2020, no. 10795/14, paras 33 ff.; *Văcean v. Romania*, judgment of 16 November 2021, no. 47695/14, paras 30 ff. For an early overview, see Robert Uerpmann-Wittzack and Magdalena Jankowska-Gilberg, 'Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet,' Multimedia und Recht 2008, 83–89, with further references.

16 See ECtHR, *Rotaru v. Romania*, judgment of 4 May 2000, no. 28341/95, paras 40 ff. The EU Charter of Fundamental Rights, however, guarantees these two rights separately in Articles 7 and 8.

17 See Human Rights Council, A/HRC/17/26, 16 May 2011, A/HRC/20/L.13, 29 June 2012 and A/HRC/28/L.27, 24 March 2015.

18 See the Reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011, para. 55, A/HRC/23/40, 17 April 2013, para. 24, and the Report of the Special Rapporteur on the right to privacy, A/HRC/31/64, 14 November 2016, para. 8.

19 UNGA Res 68/167 of 18 December 2013, A/RES/68/167, para. 3; UNGA Res 69/166 of 18 December 2014, A/RES/69/166, paras 3 ff.

20 OHCHR, A/HRC/27/37, 30 June 2014, paras 12 ff.

21 Human Rights Committee, 'General Comment No. 16,' 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I), para. 10 and 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, paras 12, 15, 39, 43.

22 FRA, 'Report on surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union' (Luxembourg: Publications Office of the European Union, 2015), *passim*. Yet, it has to be underlined that the

(CJEU)[23] and the ECtHR[24] – to name but a few – have all consistently and repeatedly emphasised the right to privacy in the online communication. In general, it can be said that both communication rights and the right to enjoy a private life apply to the same extent in the online as in the offline world.[25] However, this fact is not a surprising innovation to the international human rights regime, but rather a usual dynamic interpretation of existing human rights guarantees in the sense of Article 31(3) of the 1969 Vienna Convention on the Law of Treaties.[26]

Yet, the effects of the internet and the growing digitalisation of societies on the general dogmatic aspects of human rights treaties have not yet been thoroughly investigated. Most of the scholarly contributions that deal with the matter focus on selected human rights perspectives only, e.g., on those of children and adolescents, or on selected human rights topics such as, e.g., data protection without going into the overarching challenges of digitalisation for the dogmatic structures of the human rights

---

Agency's mandate only extends to carrying out studies on fundamental rights issues in so far as they fall into the scope of EU law.

23 See, e.g., CJEU, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, judgment of 9 November 2010, cases no. C-92/09 and C-93/09, ECLI:EU:C:2010:662, paras 49, 52; *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, judgment of 8 April 2014, cases no. C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 29; *EU-Canada PNR Agreement*, opinion 1/15 of 26 July 2017, ECLI:EU:C:2017:592, paras 122–123; *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems No. 2)*, case C-311/18, judgment of 16 July 2020, ECLI:EU:C:2020:559, para. 170; *La Quadrature du Net and Others v. Premier Ministre and Others*, cases C-511/18 et al., judgment of 6 October 2020, ECLI:EU:C:2020:791, paras 117, 130.

24 See, e.g., ECtHR, *Weber and Saravia v. Germany,* judgment of 29 June 2006, no. 54934/00, para. 77; *S. and Marper v. The United Kingdom*, judgment of 4 December 2008, nos. 30562/04 and 30566/04, paras 66–7; *Iordachi and Others v. Moldova*, judgment of 10 February 2009, no. 25198/02, para. 29; *Kennedy v. The United Kingdom*, judgment of 18 May 2010, no. 26839/05, para. 118; *Ben Faiza v. France*, judgment of 8 February 2018, no. 31446/12, paras 53 ff.; *Breyer v. Germany*, judgment of 30 January 2020, no. 50001/12, paras 74 ff.; *Văcean* (n. 15), paras 43 ff.

25 See Matthias C. Kettemann, 'Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühlings,' HJIL 72 (2012), 469–482 (472–475); David P. Fidler, 'Cyberspace and Human Rights' in: Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing 2015), 94–117 (99–103).

26 Stefanie Schmahl, 'Intelligence and Human Rights' in: Jan-Hendrik Dietrich and Satish Sule (eds), *Intelligence Law and Policies in Europe* (München: Beck/Nomos/Hart 2019), 291–334 (para. 31).

system as a whole. Therefore, an attempt will be made to shed a first light on the main challenges that typically arise when trying to determine the structural relationship between international human rights law on the one hand and behaviours of individuals in the digital environment and of intelligent, human-like machines on the other. These main challenges, outlined in section II., include specific structural features such as the existence or non-existence of a right to access the Internet (1.) and of new digital spheres of human rights (2.), as well as more general human rights aspects such as the determination and possible extension of both duty-bearers and rights-holders (3., 4. and 7.), the extraterritorial application of human rights (5.) and the fight against new discrimination problems due to the growing use of algorithms (6.).

Of course, this contribution cannot conclusively determine the systematic relationship between digitalisation and international human rights either. Too many aspects are technologically, ethically and legally in flux. Moreover, the relevant constellations are so varied that it is impossible to give a 'one-size-fits-all' answer. Nevertheless, initial sketches of ideas shall be presented to what extent the digital environment offers opportunities for the realisation of human rights on the one hand and to what extent it critically challenges the functioning of the international human rights regime on the other.

II. Effects of the Digitalisation of Societies on the General Requirements of Human Rights Treaties

1. Right to Access the Internet

The first fundamental question that needs to be answered is whether there is a human right to access the Internet. This right may be understood in twofold ways, in that it entails not only access to the Internet in terms of infrastructure, availability of devices and Internet connection but also in terms of acquiring digital skills. As regards the former, there is no doubt that without infrastructural and unhindered access to the Internet and its content, people will not be able to take part in the potential of the digitalisation of societies.[27] In Africa, for instance, less than 20 % of the populati-

27 Matthias C. Kettemann, 'Menschenrechte im Multistakeholder-Zeitalter: Mehr Demokratie für das Internet?,' Zeitschrift für Menschenrechte 10 (2016), 24–36 (24).

on has access to the Internet and digital devices. In particular, women and people living in rural areas in the African continent are excluded from Internet access and thus from the knowledge and understanding that is conveyed online.[28] Also, in European countries, the digital infrastructure and the quality of the Internet connection is unevenly distributed. In rural areas in Germany, for instance, Internet access, if available at all, is often cumbersome, slow and unstable. Especially in times of the Covid19 pandemic, in which digital home schooling was deemed necessary to keep the interpersonal distance for medical reasons, the lack of expansion of the digital infrastructure in rural areas has had disadvantageous effects on the rights of the child to education. It widened the knowledge gap and existing inequalities for children living in rural areas and in vulnerable situations.

In addition to providing the necessary digital infrastructure, learning digital skills is also indispensable for effective participation in the digitalised society. The Committee on Economic, Social and Cultural Rights (CESCR Committee) has pointed out that predominantly older persons and persons with low levels of education and income do not have access to the Internet for financial reasons or have limited digital skills. They are therefore hindered from fully enjoying their human rights to information and education.[29] In particular, access to the Internet is of crucial importance for marginalised and minority groups in order to manifest and elaborate their personal and cultural identity.[30] Therefore, the Committee on the Elimination of Discrimination against Women (CEDAW Committee) rightly stresses that States parties are obliged to ensure access to and knowledge of the Internet and other information and communications technologies in order to improve women's education and access to justice systems at all levels.[31] The recommendations of the CRC Committee and

28 See African Union, 'Déclaration de l'Union Africaine sur la gouvernance de l'internet et le développement de l'économie numérique en Afrique,' Assembly/AU/Decl. 3(XXX), 29 January 2018, Recital no. 5.

29 CESCR Committee, 'Concluding Observations: Estonia,' 27 March 2019, E/C.12/EST/CO/3, para. 52.

30 CESCR Committee, 'General Comment No. 21,' 21 December 2009, E/C.12/GC/21, para. 32. Similarly, with particular regard to the rights of persons with disabilities, Dörte Busch 'Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention', Zeitschrift für europäisches Sozial- und Arbeitsrecht 20 (2021), 484-492 (485 ff.).

31 See CEDAW Committee, 'General Recommendation No. 33,' 3 August 2015, CEDAW/C/GC/33, para. 17d. Similarly, IACtHR, *Escher et al. v. Brazil*, judgment of 6 July 2009, paras 43–46.

the CESCR Committee point to a similar direction.[32] In fact, Internet access and digital skills are not only a prerequisite for exercising freedom of communication but also an essential starting point for exercising other rights. Access to the Internet is today a 'core utility' and can be regarded as an 'essential infrastructure for communities.'[33] Against this background, the UN Human Rights Council and various human rights monitoring bodies repeatedly call on States to promote and facilitate (infrastructural and learned) access to the Internet for everyone.[34]

However, a State's obligation to provide access to the Internet that can be enforced directly under human rights law is not existent.[35] The human rights monitoring bodies focus solely on an obligation of conduct, not of result. From a doctrinal perspective, an obligation of result could be justified, for example, as a derivative right of the States' obligation to guarantee everyone a decent subsistence level which, today, might include the access to digital infrastructure. An obligation of result could also be construed as being a legal precondition for exercising other rights.[36] The Community Court of Justice of the Economic Community of the West African States (CCJ ECOWAS) emphasises that access to the Internet is a derivative right within the context of the right to freedom of expression and should be treated as an integral part of the right.[37] However, the Court itself considers that restrictions, even a complete shutdown of the Internet, are permissible under certain conditions.[38]

Similarly, the CESCR Committee only recommends that States parties ensure that digital assistance is easily available for those who have neither access to the Internet nor the digital skills to access information and

32 See, e.g., CRC Committee, 'General Comment No. 13,' 18 April 2011, CRC/C/GC/13, para. 8; CESCR Committee, 'Concluding Observations: Estonia,' 27 March 2019, E/C.12/EST/CO/3, para. 53 and 'General Comment No. 25,' 30 April 2020, E/C.12/GC/25, para. 16.

33 Kettemann (n. 27), 27.

34 See, e.g., Human Rights Council, 16 July 2012, HRC/RES/20/8, para. 3; ACHPR, 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa,' 4 November 2016, ACHPR/Res. 362(LIX), para. 1; Human Rights Committee, 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, para. 15.

35 See Fidler (n. 25), 106–107.

36 Similarly, Kettemann (n. 27), 25–26.

37 CCJ ECOWAS, *Amnesty International Togo et al. v. The Togolese Republic*, judgment of 25 June 2020, no. ECW/CCJ/JUD/09/20, para. 38.

38 CCJ ECOWAS, *Amnesty International Togo et al* (n. 37), para. 45.

communications technology based public services.[39] It further mentions the importance of Internet access for all those who seek assistance, employment and opportunities to develop their skills and calls upon States to facilitate access to the Internet, particularly for marginalised and disadvantaged groups.[40] But the CESCR Committee makes all these requirements dependent on available resources. Also, the legally non-binding 2030 Agenda for Sustainable Development focuses solely on an obligation of conduct by stating that universal and affordable access to information and communications technology, including the Internet, should significantly increase.[41] In sum, the States are called upon to adopt laws, policies and other measures in cooperation with all relevant stakeholders and make the best possible use of their resources to provide universal, equitable, affordable and meaningful access to the Internet without discrimination.

Conversely, however, it does not follow from the fundamental obligation of States to ensure access to the Internet on the basis of available resources that the individual is obliged to use the Internet or digital technologies in all circumstances. In this respect, negative freedom gives the individual, in principle, the right to abstain from any form of participation in a digital society. This means that there must generally be no legal, soft law or *de facto* obligations for the use of digital tools.[42] The right to self-determination and autonomy presupposes that every individual must have the possibility not to participate in the virtual world and to lead their lives exclusively in an analogous way. Thus, analogous options for, e.g., purchasing tickets or political elections, must continue to be available alongside online alternatives such as blockchain technology.[43] The provision and the use of analogue devices remains even possible in exceptional situations, like the Covid19 pandemic, which demands distance between people for medical reasons. For example, political elections can be organised as postal votes; and tickets can be ordered by phone and sent by conventional mail. At least at present, when not all people, in particular

39 CESCR Committee, 'Concluding Observations: Estonia,' 27 March 2019, E/C.12/EST/CO/3, para. 53.

40 CESCR Committee, 'Concluding Observations: Djibouti,' 30 December 2013, E/C.12/DJI/CO/1–2, para. 38.

41 UNGA Res 70/1 of 25 September 2015, A/RES/70/1, 21 October 2015, Goal 9c.

42 In regards to this aspect, see Wenguang Yu, 'Verlagerung von Normsetzungskompetenzen im Internet unter besonderer Berücksichtigung der Cybersecurity Standards,' DÖV 73 (2020), 161–172 (162).

43 As regards the use of the blockchain technology for political elections, see Tobias Mast, 'Schöne neue Wahl – Zu den Versprechen der Blockchain-Technologie für demokratische Wahlen,' JZ 76 (2021), 237–246.

older persons or persons with disabilities, are yet able or willing to use digital devices, any mandatory use of online tools would contradict the basic human rights of equality and freedom. Only in the case of distance learning for children and adolescents in times of pandemics may different parameters apply due to the compulsory character of schooling. But here, too, ventilation systems could be installed in classrooms and based on this, intelligent forms of face-to-face teaching could be organised in small groups or in alternating lessons in order to alleviate the hardships of purely digital lessons for children and parents.

2. *New Digital Spheres of Human Rights*

If individuals make use of their freedoms in a virtual form, a second challenge that must be resolved consists in whether all or only some human rights have a specific digital sphere of protection. With regard to freedom of expression and information and the protection of private life, the digital sphere has already been developed dynamically on several occasions by both international courts and human rights expert committees.[44] However, it is less clear whether this finding extends to other or even all human rights. This becomes relevant, for instance, when addressing freedom of assembly, which is primarily tailored to the physical presence of the participants.

It is debatable whether freedom of assembly can be transferred to political actions on online platforms, video conferences, or Internet fora that call for discussion, e.g., under a certain hashtag. Some scholars deny the relevance of the freedom of assembly for virtual gatherings with a view to the lack of physical danger emanating from such assemblies.[45] Another argument often put forward in this context is that there is no protection gap if freedom of assembly does not cover virtual assemblies since all

44 See the references in notes 8–24. Further see Udo Di Fabio, *Grundrechtsgeltung in digitalen Systemen* (München: Beck 2016), 83 ff.

45 See, e.g., Michael Kniesel, 'Versammlungs- und Demonstrationsfreiheit – Entwicklung des Versammlungsrechts seit 1996,' NJW 53 (2000), 2857–2866 (2860); Sebastian Hoffmanns, 'Die 'Lufthansa-Blockade' 2001 – eine (strafbare) Online-Demonstration?,' Zeitschrift für Internationale Strafrechtsdogmatik 7 (2012), 409–414 (412–413).

relevant actions may be sufficiently secured by freedom of expression and information.[46] However, this line of reasoning overlooks three aspects.

Firstly, online assemblies go beyond expressing one's opinions; they rather resemble a collective engagement in building and sharing views and opinions. Therefore, the UN Special Rapporteur on freedom of assembly and association rightly appeals to the States to recognise that 'the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the Internet.'[47] Recently, the UN Human Rights Committee has explicitly concurred with this view.[48]

Secondly, there is a relatively high risk of interference by State authorities or third private parties in this virtual engagement. The UN Human Rights Committee stresses that States parties must not block or hinder Internet connectivity in relation to peaceful assemblies.[49] The same applies to geo-targeted or technology-specific interference with connectivity or access to content. States should ensure that the activities of Internet service providers do not unduly restrict online assemblies.[50]

Thirdly, virtual gatherings harbour considerable dangers if the inherent group dynamic leads to an anonymous 'shit storm' that violates the personal rights of others.[51] If the participants in a virtual meeting slow down or block the services of an external server through distributed denial of service attacks, they can threaten the property of third parties.[52] The UN Human Rights Committee has therefore made clear that virtual gatherings

---

46 See, e.g., Jürgen Bröhmer, 'Versammlungs- und Vereinigungsfreiheit' in: Oliver Dörr, Rainer Grote and Thilo Marauhn (eds), *EMRK/GG, Konkordanzkommentar* (Tübingen: Mohr Siebeck, 2nd. edn 2013), 1161–1232 (para. 25).

47 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/20/27, 21 May 2011, para. 84k. Similarly, Christian Möhlen, 'Das Recht auf Versammlungsfreiheit im Internet – Anwendbarkeit eines klassischen Menschenrechts auf neue digitale Kommunikations- und Protestformen,' Multimedia und Recht 2013, 227–230.

48 Human Rights Committee, 'General Comment No. 37,' 27 July 2020, CCPR/C/GC/37, para. 34.

49 Human Rights Committee, 'Concluding Observations: Cameroon,' 30 November 2017, CCPR/C/CMR/CO/5, paras 41–42.

50 Human Rights Committee, 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, para. 34 and 'General Comment No. 37,' 27 July 2020, CCPR/C/GC/37, para. 34.

51 See Stephan Pötters and Christoph Werkmeister, 'Grundrechtsschutz im Internetzeitalter,' JURA 35 (2013), 5–12 (9); Corinna Nitsch and Michael Frey, 'Grundrechte im Zeitalter der Digitalisierung – Die digitale Sphäre der Versammlungsfreiheit,' DVBl. 135 (2020), 1054–1056 (1055).

52 See Nitsch and Frey (n. 51), 1056.

must be subject to the same restrictions as analogue assemblies. In the case of serious threat potential, Internet observations and isolated geo-targeted blocking by State authorities can be considered permissible under certain circumstances.[53]

These thoughts on the digital sphere of protection of the freedom of peaceful assembly can be transferred to other human rights, which typically required a physical presence in the 'pre-digital era.' As a rule, the interpretation and application of human rights can be adapted to the digital challenges by means of a dynamic interpretation. This is, in particular, made clear by General Comment No. 25 of the CRC Committee, which covers not only the non-physical human rights such as access to information and freedom of expression but also rights that, as a rule, presuppose a physical presence such as freedom of association, access to health services and to culture, leisure and play. The CRC Committee gives these rights a plausible interpretation in the light of the digital environment.[54] In a similar way, business freedom and property rights also claim validity on the Internet and in a digital environment.[55]

However, these human rights are coming under strong pressure from the opensource movement, which considers the assertion of property rights in intellectual services as an attack on the freedom of the Internet. Also, search engines and social networks growingly take advantage of the works and achievements of others. Consequently, the authors concerned see themselves deprived of the income from their intellectual work, on which they make a living.[56] The discussion about the EU Copyright Directive[57] has shown how heated the debate is and what negative consequences an all-encompassing 'free mentality' can have for the liberal human rights system.[58]

53 Human Rights Committee, 'General Comment No. 34,' 12 September 2011, CCPR/C/GC/34, para. 34.

54 See CRC Committee, 'General Comment No. 25,' 2 March 2021, CRC/C/GC/25, paras 50 ff.

55 See Christine Langenfeld, 'Der Schutz freier Kommunikationsräume in der digitalen Welt – Eine Gedankenskizze,' ZEuS 24 (2021), 33–42 (37).

56 Ibid., 37.

57 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ 2019 L 130/92.

58 Di Fabio (n. 44), 79.

3. Extension of Duty-Bearers of Human Rights

It is well-known that threats to individual privacy no longer emanate exclusively from State authorities, but increasingly also from private third parties, above all from globally operating technology companies and the digital industry.[59] The right to privacy is probably the one where most cases of indirect third-party effects occur today, for example, when employers or companies resort to clandestine video surveillance and Internet tracking,[60] when Facebook and Cambridge Analytica siphon off vast amounts of data from their users without informed consent and prior authorisation,[61] or where a search engine operator includes an automatised reference and information system contained in a list of results displayed following a search conducted on the basis of an individual's name.[62] Also, the employment of big data and new technologies by State and third party agencies and the emergence of 'smart cities,' that include surveillance technologies in public spaces and further artificial intelligence tools to combat crime and terrorism, pose significant risks to human rights.[63]

---

59 See Hans-Jürgen Papier, 'Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft,' NJW 70 (2017), 3025–3031 (3026).

60 See, e.g., Klaus Herrmann and Michael Soiné, 'Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz,' NJW 64 (2011), 2922–2928 (2927); Jobst-Hubertus Bauer and Mareike Schansker, '(Heimliche) Videoüberwachung durch den Arbeitgeber,' NJW 65 (2012), 3537 (3538 ff.); Viktoria Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data,' CML Rev 57 (2020), 161–190 (171 ff.).

61 An illustrative case in that regard is CJEU, *Schrems No. 2* (n. 23), paras 2 ff. See further Walter Frenz, 'Anmerkung zu EuGH C-311/18: Schrems II,' DVBl. 135 (2020), 1270–1272 (1270); Alexander Golland, 'Datenschutzrechtliche Anforderungen an internationale Datentransfers,' NJW 73 (2020), 2593–2596; Thorsten Schröder, 'Wie Facebook über sich selbst stolperte,' ZEIT Online, 20 March 2018, available at: http://www.zeit.de/wirtschaft/2018-03/facebook-datenmissbrauch-cambridge-analytica-mark-zuckerberg-politik.

62 See CJEU, *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*, judgment of 13 May 2014, case C-131/12, ECLI:EU:C:2014:317, paras 80 ff.; *Bolagsupplysningen OU and Ingrid Ilsjan v. Svensk Handel AB*, judgment of 17 October 2017, case C-194/16, ECLI:EU:C:2017:766, para. 48; *Google LLC v. CNIL*, judgment of 24 September 2019, case C-507/17, ECLI:EU:C:2019:772, para. 56. See also John W. Kropf, 'Google Spain SL v. Agencia Española de Protección de Datos (AEPD),' AJIL 108 (2014), 502–509; Monika Zalnieriute, 'Google LLC v. Commission nationale de l'informatique et des libertés (CNIL),' AJIL 114 (2020), 261–267.

63 Lorna McGregor, 'Looking to the Future: The Scope, Value and Operationalization of International Human Rights Law,' Vand J Transnat'l L. 52 (2019), 1281–

Yet, it is still the State which remains the duty-bearer within international human rights law. The duty to ensure compliance with human rights treaties primarily establishes a direct obligation incumbent on the Contracting States, since it is the States' consents that underpin international law's content.[64] However, this duty contains a further obligation upon States parties to ensure that non-governmental or private service providers, such as multinational technology corporations, act in accordance with the provisions of the conventions. This means that States are required to put in place a framework that prevents human rights violations from occurring, establish monitoring mechanisms as safeguards and hold those responsible to account.[65] These obligations apply directly to State actions or omissions and, through the duty to protect human rights on the one hand and the due diligence principle on the other, the States must also protect individuals from harm by private third parties, including business enterprises.[66] In other words, human rights treaties create indirect obligations, or indirect horizontal effects, for non-State actors, by establishing (direct) positive duties on States parties.[67] The transfer of powers to private service providers or private institutions must not lead to a reduction of protection below the level required by the conventions. For instance, the CEDAW Committee recurrently underlines that States parties have to take measures, including the adoption of legislation and national action plans, to protect women from Internet crimes and other misdemeanours

1314 (1303); Alexander Kriebitz and Christoph Lütge, 'Artificial Intelligence and Human Rights: A Business Ethical Assessment,' Business and Human Rights Journal 5 (2020), 84–104 (85).

64 Jay Butler, 'The Corporate Keepers of International Law,' AJIL 114 (2020), 189–218 (194).

65 See Carlos Manuel Vázquez, 'Direct vs. Indirect Obligations of Corporations Under International Law,' Colum J Transnat'l L. 54 (2005), 927–959 (930).

66 See Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability,' ICLQ 68 (2019), 309–343 (311–312).

67 See, e.g., CRC Committee, 'General Comment No. 5,' 27 November 2003, CRC/GC/2003/5, paras 43, 56, 'General Comment No. 15,' 17 April 2013, CRC/GC/C/16, para. 8 and General Comment No. 21, 21 June 2017, CRC/C/GC/21, para. 15. See also CESCR Committee, 'General Comment No. 14,' 11 August 2000, E/C.12/2000/4, para. 42. As regards the regional level, see, e.g., Matthias Klatt, 'Positive Obligations under the European Convention of Human Rights,' HRLJ 71 (2011), 691–718; Laurens Lavrysen, 'Positive Obligations in the Jurisprudence of the Inter-American Court of Human Rights,' Inter-American and European Human Rights Journal 7 (2014), 94–115.

that women experience online.[68] Both the Committee on the Elimination of Racial Discrimination (CERD Committee) and the CRC Committee point out that States parties should take resolute action to combat hate speech, cyberbullying, and racial as well as sexual violence on the Internet and other electronic communications networks.[69] The CRC Committee further stresses that all human rights provisions must be respected in legislation and policy development, including the private and business sector.[70] While the implementation is primarily the responsibility of States parties, the duty to respect, to protect and to fulfil human rights extends indirectly beyond the State and State-controlled services. States parties are demanded to enact laws and policies directed to private institutions and other non-State services in order to ensure that their activities and operations do not have adverse human rights implications.[71]

As important as these requirements are, they also have shortcomings in the Internet context. The transnational, instantaneous nature of Internet communications makes it difficult for governments to directly influence the information entering or leaving a country, while at the same time, the power of the private Internet providers and search engine operators, which control this flow of information, is increasing.[72] This form of governance over digital platforms is problematic for a human rights system that treats human rights solely as a government responsibility. As demonstrated, most international human rights law is concerned with the obligations of States to provide remedies for the abuse of human rights by businesses and other non-State actors. However, such frameworks do not easily apply

---

68 See CEDAW Committee, 'General Recommendation No. 33,' 3 August 2015, CEDAW/C/GC/33, para. 51e, 'General Recommendation No. 35,' 26 July 2017, CEDAW/C/GC/35, para. 30, and 'Concluding Observations: Venezuela,' 11 January 2018, CEDAW/C/VEN/CO/7–8/Add.1, para. 7.

69 See CERD Committee, 'General Recommendation No. 35,' 26 September 2013, CERD/C/GC/35, paras 7, 15, 39 and 42, and 'Concluding Observations: Iceland,' 18 September 2019, CERD/C/ISL/CO/21–23, paras 13–14; CRC Committee, 'General Comment No. 13,' 18 April 2011, CRC/C/GC/13, paras 21, 31.

70 CRC Committee, 'General Comment No. 16,' 17 April 2013 CRC/C/GC/16, para. 8.

71 CRC Committee, 'General Comment No. 16,' 17 April 2013, CRC/C/GC/16, para. 5; Julia Sloth-Nielsen, 'Monitoring and Implementation of Children's Rights' in: Ursula Kilkelly and Ton Liefaard (eds), *International Human Rights of Children* (Cham: Springer 2019), 31–64 (52).

72 See Emily B. Laidlaw, *Regulating Speech in Cyberspace. Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge: Cambridge University Press 2015), 83. Similarly, Josef Drexl, 'Bedrohung der Meinungsvielfalt durch Algorithmen,' Zeitschrift für Urheber- und Medienrecht 61 (2017), 529–543 (536).

to international digital enterprises and technology companies, which are often not the culprits themselves but enable or gatekeep the wrongdoing of others. Furthermore, States have to ensure that there is no risk for the maintenance of the principle of non-discrimination by the increasing use of algorithms. They have to secure that policies and practice are in place to identify and assess any actual or potential dangers to human rights.[73]

In this grey area of governance of Internet gatekeepers, search engine operators and technology companies, the work of the former Special Representative of the UN Secretary-General on the issue of human rights and businesses, John Ruggie, emerges as important, because it seeks to bridge the governance gap between the human rights impact of businesses and the historical focus of human rights law on States.[74] Ruggie's attempt to apply State-like human rights obligations to companies in his 2011 Report on Guiding Principles on Business and Human Rights[75] was strongly endorsed by the UN Human Rights Council, entrenching them as the authoritative global reference point for business and human rights.[76] The extension of the scope of human rights standards to a digital sphere with enlarged responsibilities of digital companies would therefore have to entail a corresponding extension of the duty to protect, in particular the possibility of horizontal interventions by market-dominant companies and the recognition of a direct third-party effect of human rights.[77] It is not a coincidence that, under Principles 11 and 13 of the UN Guiding Principles on Business and Human Rights, corporations, including technology com-

73 McGregor, Murray and Ng (n. 66), 329. But see also the rather reserved assessment regarding German constitutional law by Jürgen Kühling, 'Die Verantwortung der Medienintermediäre für die demokratische Diskursvielfalt', JZ 76 (2021), 529-538 (534).

74 Rightly so, Laidlaw (n. 72), 90. See also Kriebitz and Lütge (n. 63), 88.

75 Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises John Ruggie, 'Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework,' A/HRC/17/31, 21 March 2011, paras 1–16.

76 Human Rights Council, 'Human rights and transnational corporations and other business enterprises,' A/HRC/RES/17/4, 16 June 2011, para. 1. See also Laidlaw (n. 72), 91.

77 Christian Hoffmann, Sönke Schulz and Kim Corinna Borchers, 'Grundrechtliche Wirkungsdimensionen im digitalen Raum,' Multimedia und Recht 2014, 89–95 (92); Butler (n. 64), 201. See also, in a more general way, Lottie Lane, 'The Horizontal Effect of International Human Rights Law in Practice,' European Journal of Comparative Law and Governance 5 (2018), 5–88 (16 ff.).

panies, must not only refrain from human rights violations, but also avoid adverse human rights impacts through their business activities.

As a result of their outstanding market position *vis-à-vis* citizens, private companies often act in the digital sector as powerfully as the State and can considerably restrict, lead or manipulate citizen's behaviour.[78] In the famous *Bosman* ruling regarding the free movement of workers, the CJEU recognised this role of certain private actors such as sports associations.[79] The Court has recently transferred this argument *mutatis mutandis* to the role of technology companies regarding the individual's 'right to be forgotten' and the ensuing obligation of the search engine operators, such as Google, to carry out de-referencing requests on versions of their search engine, provided that the data subject's right to privacy is adequately balanced against the right to freedom of information.[80] This view of the CJEU takes into account the limited ability of States to transfer the standards of international human rights law to transnationally operating digital corporations, by establishing direct horizontal effects of European fundamental rights.[81]

Another possibility is, of course, that States simply close the regulatory gaps that exist for technology companies by treating private governance as a modality of governance that must be strictly embedded in a framework of the rule of law.[82] This is the path taken by the 2017 German Network Enforcement Act, last modified in June 2021,[83] which forms part and is the

78 McGregor (n. 63), 1305; Utz Schliesky, 'Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat,' NVwZ 38 (2019), 693–701 (694). For this reason, the (German) Federal Court of Justice has subjected the social media platforms active in Germany to an increased indirect third-party effect of fundamental rights, see Federal Court of Justice, judgment of 29 July 2021, III ZR 179/20.

79 CJEU, *Union royale belge des sociétés de football association ASBL and Others v. Jean-Marc Bosman*, judgment of 15 December 1995, case C-269/92, ECLI:EU:C:1995:463, paras 82–87.

80 CJEU, *Google Spain* (n. 62), paras 96–99; *Google LLC v. CNIL* (n. 62), para. 72. Similar arguments can be found in CJEU, *Schrems No. 2* (n. 23), paras 85–86.

81 Butler (n. 64), 208–209.

82 Nicholas Tsagourias, 'The Rule of Law in Cyberspace: A Hybrid and Networked Concept?,' HJIL 80 (2020), 433–451 (447).

83 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) of 1 September 2017, Bundesgesetzblatt 2017 I, 3352, last modified on 3 June 2021 in: Bundesgesetzblatt 2021 I, 1436. For more detail, see Matthias Cornils, 'Präzisierung, Vervollständigung und Erweiterung: Die Änderungen des Netzwerkdurchsetzungsgesetzes 2021', NJW 74 (2021), 2465-2471. The UK's Online Safety Bill, published by the UK Government on 12

result of the State's duty to protect human rights. The German Network Enforcement Act aims to ensure that Internet platforms delete or block illegal or manifestly unlawful content – in particular in cases where the private invader remains anonymous vis-à-vis the victim. In a similar way, the Digital Services Act proposed by the European Commission on 15 December 2020[84] aims at encompassing a set of new rules applicable to online intermediaries and platforms across the whole European Union to create a safe digital space. The rules specified in the proposal primarily establish due diligence obligations for online intermediaries and online platforms to, *inter alia*, take measures against abusive notices and counter-notices and to report of suspicious criminal offences. These paths are preferable to establishing a direct human rights obligation on the part of technology companies, as they do not call into question the dogmatics and the liberal character of international human rights protection. In this respect, it is important to note that the operation of an online platform by a technology company is also protected by the freedom of expression, since it is the online platform that enables the exchange of opinions between people who do not know each other.[85]

4. Modes of Protecting and Counteracting Anonymity in the Digital Sphere

This fact leads to the next challenge for international human rights protection in the age of digitalisation, which is anonymity, i.e., the concealment of the identity of actors and their actions. It is true that anonymity has

---

May 2021, points to a similar direction. For more detail see Edina Harbinja, 'The UK's Online Safety Bill: Safe, Harmful, Unworkable?,' Verfassungsblog, 18 May 2021, DOI: https://dx.doi.org/10.17176/20210518-170138-0" \t

84 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final. For more detail, see, e.g., Michael Denga, 'Plattformregulierung durch europäische Werte: Zur Bindung von Meinungsplattformen an EU-Grundrechte,' EuR 56 (2021), 569-595 (579 ff.); Wolfgang Beck, 'Der Entwurf des Digital Services Act,' DVBl. 136 (2021), 1000-1005 (1000 ff.); Nico Gielen and Steffen Uphues, 'Digital Markets Act und Digital Services Act,' EuZW 32 (2021), 627-637 (632 ff.); Martin Eifert, Axel Metzger, Heike Schweitzer and Gerhard Wagner, 'Taming the Giants: The DMA/DSA Package,' CMLRev. 58 (2021), 987-1028 (1008 ff.).

85 Clearly so, (German) Federal Court of Justice, judgment of 27 January 2022, III ZR 3/21, para. 37; further see Stephanie Schiedermair/Johannes Weil, 'Online-Intermediäre als Träger der Meinungsfreiheit,' DÖV 75 (2022), 305-314.

always existed in the offline world. It was and is mostly used in order to avoid responsibility for an action, to reduce the risk of sanctions or to eliminate them altogether.[86]

The digitalisation of the living environment has not fundamentally modified traditional anonymous actions, but it has noticeably dynamized them. This is mainly due to the fact that the Internet is changing the time barriers, physical and spatial distances and financial costs of all activities, adding ubiquitous, simultaneous and immediately noticeable effects.[87] Internet users often make a conscious choice to communicate or use online activities anonymously, by not using full or real names, suppressing their IP addresses or even using subtle obfuscation techniques.[88] It is no coincidence that the Internet phenomenon 'Anonymous' – known from the Guy Fawkes mask – has become a political icon of a network-based activism that campaigns for Wikileaks and against racism and child pornography.[89] In his work '*L'art de la révolte*,' the French philosopher and sociologist Geoffroy de Lagasnerie transfigured this development towards a culture of anonymity into a political world citizenship that constructs a new legal order at the grassroots level.[90] This postulate must be clearly rejected. A democratic State based on the rule of law cannot be constituted by a collection of people who, due to their anonymity, evade any individual or democratic responsibility.[91] Furthermore, there is a high risk that information will be manipulated by artificial intelligence's filtering, which

86 See Jens Kersten, 'Anonymität in der liberalen Demokratie,' JuS 57 (2017), 193–203 (193).

87 See Volker Boehme-Neßler, 'Die Macht der Algorithmen und die Ohnmacht des Rechts,' NJW 70 (2017), 3031–3037 (3032); Thorsten Thiel, 'Anonymität und der digitale Strukturwandel der Öffentlichkeit,' Zeitschrift für Menschenrechte 10 (2016), 7–22 (13 ff.); Johannes Unterreitmeier, 'Das Internet als Herausforderung der inneren Sicherheit,' BayVBl. 2021, 689-696 (691 ff.).

88 Instructive analysis by Duncan B. Hollis, 'An e-SOS for Cyberspace,' Harv. Int'l. L. J. 52 (2011), 373–432 (397 ff.); Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity,' AJIL 110 (2016), 425–479 (435, 458–459).

89 See, e.g., Frédéric Bardeau and Nicolas Danet (translation by Bernard Schmidt), *Anonymous: Von der Spaßbewegung zur Medienguerilla* (Münster: Unrast 2012); Jacques de Saint Victor, *Die Antipolitischen* (Hamburg: Hamburger Edition 2015).

90 Geoffroy de Lagasnerie, *L'art de la révolte: Snowden, Assange, Manning* (Paris: Fayard 2015), 80 ff.

91 See Kersten (n. 86), 194; Schliesky (n. 78), 697 ff.; Gabriele Buchholtz, 'Demokratie und Teilhabe in der digitalen Zeit,' DÖV 70 (2017), 1009–1016 (1009).

could change the political discourse's direction and suppress parts of the opinion.[92]

However, different requirements are likely to apply to the protection of human rights. The right to private life gives everyone a subjective right to anonymity.[93] Every individual is generally free to decide on the reason, the mode and the duration of his or her identifiability.[94] For example, real names, private photos and personal data may, as a rule, only be published with the consent of the rights-holder.[95] States are therefore required to respect and guarantee the privacy and security of communication on the Internet and to protect the personal rights of every individual against unlawful interference by State authorities and non-State actors effectively, which may also be reflected in the promotion of encryption technologies.[96] Anonymity in expressing opinions serves to prevent feared State reprisals and other negative effects by non-State third parties (e.g., a private employer) that could arise if the person making the statement is identified.[97] Furthermore, anonymity in the expression of opinion is intended to protect politically active citizens from the negative consequences such as self-censoring, which could produce chilling effects in the democratic debate.[98]

Yet, the right to privacy against arbitrary or unlawful State interference is not guaranteed without restriction; the main limits are the public order and national security. Only the core area of private life, which relates to human dignity, is a legal asset that is absolutely protected against State intervention. In the social sphere, in contrast, the State may identify people

92 Kriebitz and Lütge (n. 63), 100.

93 Kersten (n. 86), 195. As to the following section, see also Stefanie Schmahl, 'Anonymität im Recht: Freiheitsverbürgung oder Freiheitsgefährdung?,' JZ 73 (2018), 581–590 (583).

94 For more detail see Ansgar Ohly, 'Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?,' AfP 42 (2011), 428–438 (431–434).

95 Ohly (n. 94), 430–431.

96 Kettemann (n. 25), 475 ff.

97 See Mirko A. Wieczorek, *Persönlichkeitsrecht und Meinungsfreiheit im Internet* (Frankfurt am Main: Peter Lang 2013), 71 ff.; Jürgen Kühling, 'Im Dauerlicht der Öffentlichkeit – Freifahrt für personenbezogene Bewertungsportale!?,' NJW 68 (2015), 447–450 (448). Most recently, see also (German) Federal Court of Justice, judgment of 27 January 2022, III ZR 3/21 (n. 85), para. 51.

98 Kersten (n. 86), 196. As regards potential chilling effects under Article 10 ECHR, see Eckart Klein, 'Einwirkungen des europäischen Menschenrechtsschutzes auf Meinungsäußerungsfreiheit und Pressefreiheit,' AfP 25 (1994), 9–18 (17).

under certain circumstances.[99] On several occasions, however, European courts have repeatedly pointed out that interference by State authorities in the right to privacy and personal data protection is subject to high standards of justification and must be strictly necessary.[100] Especially in the case of secret mass surveillance, the States have to rule out the risk of abuse by issuing general, clear and precise rules governing the scope, application, purpose and objective of a measure and the timing and duration of the intervention.[101]

In multidimensional human rights situations, Internet anonymity and encryption technologies create further problems, for instance, in cases where one person's freedom of expression comes into conflict with general laws and the rights of others. It has become a commonplace that posting hateful comments or fake news on social networks under the guise of anonymity, including by Internet trolls and bots, is steadily increasing.[102] Or in other words: The rise in hate speech and bullying on the Internet clearly demonstrates the dangers (in particular for minorities) associated

99 See, e.g., ECtHR, *Rotaru v. Romania* (n. 16), para. 44; *Bărbulescu v. Romania*, judgment of 12 January 2016, no. 61496/08, paras 35 ff.; CJEU, *La Quadrature du Net* (n.), para. 135; *Privacy International*, judgment of 6 October 2020, case C-623/17, ECLI:EU:C:2020:790, paras 74 ff.; *H.K./Prokuratuur*, judgment of 2 March 2021, case C-746/18, ECLI:EU:C:2021:152, paras 29 ff.

100 See, e.g., ECtHR, *Klass v. Germany*, judgment of 6 September 1978, no. 5029/71, para. 41; *Copland v. The United Kingdom*, judgment of 3 April 2007, no. 62617/00, para. 39*; Breyer v. Germany* (n. 24), paras 83 ff.; CJEU, *Digital Rights Ireland* (n. 23), paras 50 ff.; *A./Staatsanwaltschaft Offenburg*, judgment of 21 June 2017, case C-9/16, ECLI:EU:C:2017:483, para. 63; *La Quadrature du Net* (n. 23), para. 141; *H.K./Prokuratuur* (n. 99), paras 32 ff.

101 See ECtHR *Weber and Saravia* (n. 24), paras 93–95; *Zakharov v. Russia*, judgment of 4 December 2015, no. 47143/06, para. 229; *Szabó and Vissy v. Hungary*, judgment of 12 January 2016, no. 37138/14, paras 77 and 80; *Big Brother Watch and Others v. The United Kingdom* (GC), judgment of 25 May 2021, nos. 58170/13, 62322/14 and 24960/15, paras 348 ff., para. 361; CJEU, *Digital Rights Ireland* (n. 23), paras 54 -55; *Schrems*, judgment of 6 October 2015, case C-362/14, ECLI:EU:C:2015:650, paras 91–98; *Tele2 Sverige*, judgment of 21 December 2016, cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paras 109–112, 119–125; *La Quadrature du Net* (n. 23), paras 132, 165.

102 See Dirk Heckmann, 'Persönlichkeitsschutz im Internet,' NJW 65 (2012), 2631–2635 (2632); Armin Steinbach, 'Meinungsfreiheit im postfaktischen Umfeld,' JZ 72 (2017), 653–661 (661). On the individual and societal dangers that arise from digital hatred, see Elisa Hoven and Alexandra Witting, 'Das Beleidigungsunrecht im digitalen Zeitalter,' NJW 74 (2021), 2397-2401 (2398 ff.).

with obfuscating identity in the digital world.[103] Under human rights law, States must therefore ensure that the right to anonymous expression of opinion does not apply without reservation on the Internet. It is true that freedom of expression includes both open and clandestine, even anonymous expressions of opinion.[104] In the latter cases, however, new evaluation criteria must be found for the balancing process at the level of justification.[105] It must be remembered that the individual affected by an anonymous attack cannot take effective countermeasures due to the lack of accountability of the anonymous attacker. Thus, the usual competition for the better argument, which is indispensable for free and democratic States, is led *ad absurdum*.[106] Even the guarantee of a legal remedy would be ineffective due to the concealment of the attacker's identity.[107]

Precisely for these reasons, national laws, such as the German Network Enforcement Act,[108] which oblige digital companies and social network platforms to set up complaint systems with the consequence of removing illegal online comments, are valuable measures to counter the increase in anonymous defamation on the Internet.[109] In order to uncover the identity of the commentator and to delete hate speech, the cooperation

103 See Hoffmann, Schulz and Borchers (n. 77), 89; Eva Maria Bredler and Nora Markard, 'Grundrechtsdogmatik der Beleidigungsdelikte im digitalen Raum,' JZ 76 (2021), 864-872 (865 ff.).

104 See Heckmann (n. 102), 2632; Ohly (n. 94), 436; Kersten (n. 86), 196–197.

105 Schmahl (n. 93), 584.

106 Similar assessment by Günther Wiese, 'Bewertungsportale und allgemeines Persönlichkeitsrecht,' JZ 66 (2011), 608–617 (612, 615).

107 Andreas Glaser, 'Grundrechtlicher Schutz der Ehre im Internetzeitalter,' NVwZ 31 (2012), 1432–1438 (1436).

108 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) of 1 September 2017, Bundesgesetzblatt 2017 I, 3352, last modified on 3 June 2021 in: Bundesgesetzblatt 2021 I, 1436.

109 Schmahl (n. 93), 585. Similarly, Georg Nolte, 'Hate-Speech, Fake-News, das 'Netzwerkdurchsetzungsgesetz" und Vielfaltsicherung durch Suchmaschinen,' Zeitschrift für Urheber- und Medienrecht 61 (2017), 552–565 (553 ff.); Langenfeld (n. 55), 39–40; Benjamin Raue, 'Plattformnutzungsverträge im Lichte der gesteigerten Grundrechtsbindung marktstarker sozialer Netze,' NJW 75 (2022), 209-215 (213 ff.). – The human rights conformity of the German Network Enforcement Act is very controversial, see the critical assessments by, e.g., Eike M. Frenzel, 'Aktuelles Gesetzgebungsvorhaben: Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG),' JuS 2017, 414–416; Nikolaus Guggenberger, 'Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht,' ZRP 50 (2017), 98–101; Hubertus Gersdorf, 'Hate Speech in sozialen Netzwerken,' Multimedia und Recht 2017, 439–447.

of the operators of social networks with State authorities is pivotal.[110] The communication intermediaries are easier to localise than the anonymously acting private person and thus a valid alternative strategy for the protection of human dignity and the right to privacy in cyberspace.[111] It is no coincidence that provider liability has advanced to become an essential sanctioning instrument for Internet matters in tort law, which is not only backed by the ECtHR,[112] but also by the case-law of the CJEU.[113] Here too, of course, the principle of proportionality must be strictly taken into account when partially outsourcing control mechanisms to private third parties.[114] Hate speech restrictions should never be based solely on a private company's assessment, but on legal orders from States, which also have to provide effective legal remedies against a private third party's intervention.[115]

5. Extraterritorial Application of Human Rights in the Digital Sphere

Not only domestic authorities but also intelligence agencies of foreign States and non-State actors based abroad either increasingly intercept the

---

110 See Christoph M. Giebel, 'Zivilrechtlicher Rechtsschutz gegen Cybermobbing in sozialen Netzwerken,' NJW 70 (2017), 977–983 (978 ff.). See also CERD Committee, 'General Recommendation No. 35,' 26 September 2013, CERD/C/GC/35, paras 39 and 42; 'Concluding Observations: Iceland,' 18 September 2019, CERD/C/ISL/CO/21–23, para. 14.

111 See Matthias Cornils, 'Entterritorialisierung im Kommunikationsrecht,' VVDStRL 76 (2017), 391–442 (423, 425); Martin Eifert, 'Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen,' NJW 70 (2017), 1450–1454 (1450–1451); Drexl (n. 72), 539 ff.

112 ECtHR, *Delfi AS v. Estonia*, judgment of 16 June 2015, no. 64569/09, paras 125 ff. and 159; *Magyar Tartalomszolgáltatók Egyesülete v. Hungary*, judgment of 2 February 2016, no. 22947/13, paras 62 and 69.

113 See CJEU, *Google Spain* (n. 62), paras 48 ff.

114 See the French Conseil Constitutionnel, decision of 18 June 2020, no. 2020–801 DC, ECLI: FR: CC: 2020: 2020.801.DC, paras 8 ff., which declares the French hate speech law 'Avia' partly unconstitutional for reasons of over-blocking.

115 See UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' of 9 October 2019, A/74/486, para. 47b. See also (German) Federal Court of Justice, judgment of 29 July 2021, III ZR 179/20, paras 83 ff., as regards the social media users' fundamental rights protection through procedures. Procedural rights are now being given more emphasis in the Network Enforcement Act as modified in 2021 (n. 108) and in the Commission's proposal for the Digital Services Act (n. 84), too.

communication, collect data from individuals on foreign territory, or disrupt other individual rights and legitimate interests by, for instance, posting hateful comments.[116] Against this background, the question of whether and to what extent human rights treaties can be applied extraterritorially is the fifth crucial difficulty that needs to be resolved with regard to digitalisation.

a) Extraterritorial Applicability of Human Rights Treaties to Digital Interventions by State Authorities

In principle, human rights develop their protection only in relation to encroachments that are attributable to the public authorities of the States parties. However, the attribution of such interventions to the Contracting States is not excluded if and to the extent that interventions made by a third party are carried out with the approval or tolerance of the authorities of the territorial State. Therefore, the use of communication information that is collected by foreign intelligence but passed onto domestic authorities for use must be measured against the human rights guarantees entered into by the territorial State.[117] Correspondingly, State authorities, including the intelligence services, remain in principle bound by the guarantees of the human rights treaties even if they monitor cross-border telecommunications.[118]

A more delicate question in this context is whether State authorities have to respect human rights if they only intercept foreign telecommunications abroad. Although it has not yet been conclusively clarified to what extent international human rights apply extraterritorially, there is broad agreement that they generally claim extraterritorial applicability. Both the International Court of Justice (ICJ) and the UN Human Rights Committee underline that the obligations of the International Covenant on Civil and Political Rights (ICCPR) also apply beyond the national territory of the

116 See Marko Milanović, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,' HarvIntlLJ 56 (2015), 81–146 (101); Edzard Schmidt-Jortzig, 'IT-Revolution und Datenschutz,' DÖV 71 (2018), 10–15 (13).

117 Papier (n. 59), 3029.

118 See, e.g., Stefanie Schmahl, 'Nachrichtendienste in der Völkerrechtsordnung' in: Jan-Hendrik Dietrich et al. (eds), *Nachrichtendienste im demokratischen Rechtsstaat* (Tübingen: Mohr Siebeck 2018), 21–41 (34 ff.); Milanović (n. 116), 97–98. Different view by Klaus F. Gärditz, 'Die Rechtsbindung des Bundesnachrichtendienstes bei Auslandstätigkeiten,' Die Verwaltung 48 (2015), 463–497 (472–474).

Contracting States, provided that the State concerned has an effective control over the situation abroad.[119] Contrary to Israel and the United States of America, which take the long-standing positions that the Covenant does not apply extraterritorially,[120] the human rights monitoring bodies have adopted the view that anybody directly affected by a State party's action will be regarded, for the purpose of the ICCPR, as subject to that State party's jurisdiction, regardless of the circumstances in which the power or the sufficient factual control was obtained.

The views expressed by the ICJ and the Human Rights Committee are correct. They are consistent with the principles of universality and indivisibility of human rights.[121] From the human rights perspective, an individual is entitled to protection simply because he or she is a human being, irrespective of where he or she is located and what nationality he or she is. Decisive for the applicability of the ICCPR is not the place of the violation but the relationship between the individual and the intervening State.[122] Human rights treaties never intended to grant States unchecked power to do as they pleased with individuals living outside of the country and having a different citizenship. Jurisdiction clauses were rather meant

---

119 See ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, advisory opinion of 9 July 2004, ICJ Reports 2004, 136 (paras 106–111); *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda)*, judgment of 19 December 2005, ICJ Reports 2005, 168 (para. 216); Human Rights Committee, *López Burgos v. Uruguay*, views of 29 July 1981, no. 52/1979, CCPR/C/13/D/52/1979, para. 12.3; 'General Comment No. 31,' 26 May 2004, CCPR/C/21/Rev.1/Add.13, para. 10.

120 See Human Rights Committee, 'Concluding Observations on the Third Report of Israel,' 29 July 2010, CCPR/C/ISR/CO/3, para. 5; 'Concluding Observations on the (First) Report of the United States of America,' 3 October 1995, CCPR/C/79/Add. 50, para. 19; 'Concluding Observations on the Fourth Report of the United States of America, 28 March 2014,' CCPR/C/USA/CO/4, para. 4. See also US Department of State, Office of the Legal Advisor (Harald Koh), 'Memorandum Opinion on the Geographic Scope of the ICCPR,' 19 October 2010, 12–13.

121 See ICJ, *Construction of a Wall* (n. 119), para. 109. For a fuller account see Theodor Meron, 'Extraterritoriality of Human Rights Treaties,' AJIL 89 (1995), 78–82.

122 See Rick Lawson, 'Life after Bankovic: On the Extraterritorial Application of the European Convention on Human Rights' in: Fons Coomans and Menno T Kamminga (eds), *Extraterritorial Application of Human Rights Treaties* (Antwerp: Intersentia 2004), 83–123 (86); Sarah Joseph and Adam Fletcher, 'Scope of Application' in: Daniel Moeckli, Sangeeta Shah and Sandesh Sivakumaran (eds), *International Human Rights Law* (Oxford: Oxford University Press, 3rd edn 2017), part II, chapter 6.

to prevent the responsibility of States when they are actually unable to uphold rights abroad.[123]

However, when they are in the factual position to ensure the enjoyments of rights on foreign territory, the jurisdiction clause of Article 2(1) ICCPR was not drafted to allow States to escape from their responsibilities simply on the basis of the geographical location of the affected individual.[124] The majority in legal scholarship, too, argues for the assumption that the Covenants' human rights obligations are applicable in cases where State actions are exercised extraterritorially.[125] Other UN human rights expert bodies are also unanimously in favour of the extraterritorial application of human rights treaties.[126] Finally, this line largely conforms to the case-law of the ECtHR. After a long hesitation beginning with the restrictive ruling in the *Banković Case* (2001),[127] the Court today recognises the extraterritorial applicability of the Convention rights on the basis of the principle of effective control over territory or persons[128] in order to

123 See the individual opinion of Christian Tomuschat in: Human Rights Committee, *López Burgos v. Uruguay* (n. 119), Appendix.

124 Rightly so, Tomuschat (n. 123). See also Noam Lubell, *Extraterritorial Use of Force Against Non-State Actors* (Oxford: Oxford University Press 2010), 205.

125 See, e.g., Thomas Buergenthal, 'To Respect and Ensure: State Obligations and Permissible Derogations' in: Louis Henkin (ed.), *The International Bill of Rights: the Covenant on Civil and Political Rights* (New York: Columbia University Press 1981), 72–91 (74–75); Meron (n. 121), 81; Tomuschat, *Human Rights: Between Idealism and Realism* (3rd edn, Oxford: Oxford University Press 2014), 100 ff.; Martin Weiler, 'The Right to Privacy in the Digital Age: The Commitment to Human Rights Online,' GYIL 58 (2014), 651–665 (658); Thilo Marauhn, 'Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure,' VVDStRL 74 (2015), 373–403 (380); Timo Schwander, *Extraterritoriale Wirkung von Grundrechten im Mehrebenensystem* (Berlin: Duncker & Humblot 2019), 117–129.

126 See, e.g., CEDAW Committee, *Y.W. v. Denmark*, decision of 2 March 2015, CEDAW/C/60/D/51/2013, paras 8.7; 'General Recommendation No. 35,' 26 July 2017, CEDAW/C/GC/35, para. 20; CERD Committee, 'Concluding Observations: Israel,' 27 January 2020, CERD/C/ISR/CO/17–19, paras 9, 22; CMW Committee and CRC Committee, 'Joint General Comment No. 3 and No. 20,' 16 November 2017, CMW/C/GC/3-CRC/C/GC/22, para. 12.

127 See ECtHR, *Banković and Others. v. Belgium and 16 Other Contracting States*, decision of 12 December 2001, no. 52207/99, paras 59, 61. Critical assessment by, e.g., Alexander Orakhelashvili, 'Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights,' EJIL 14 (2003), 529–568.

128 See ECtHR (Grand Chamber), *Al-Skeini v. The United Kingdom*, judgment of 7 July 2011, no. 55721/07, paras 132 ff.; *Hirsi Jamaa and Others v. Italy*, judgment of 23 February 2012, no. 27765/09, para. 172; *Mozer v. Moldavia and Russia*, judg-

prevent a vacuum in the protection of human rights.[129] In two recent decisions on surveillance measures by the secret service, in which the foreign persons concerned were not situated in the Convention State, the ECtHR has even unreservedly taken the European Convention on Human Rights as the relevant standard.[130]

Against this backdrop, the applicability of human rights treaties to digital interferences by State authorities, even if they take place extraterritorially, is now beyond question. At the national level, the (German) Federal Constitutional Court has recently recognised that the rights of the telecommunications under Articles 10(1) and 5(1) of the Basic Law, in their dimension as rights against State interference, also protect foreigners in other countries.[131] Due to technological developments, the strict concept of physical or territorial control on which the jurisdiction under Article 2(1) ICCPR and Article 1 ECHR is based, is also clearly outdated with regard to online communication.[132] Communication data typically encompass more than one person and often more than one jurisdiction. In addition, new technology on data portability frequently leads to a separation between the whereabouts of the person and the place where the privacy of the individual is invaded.[133] The choice of the virtual method must not result in the lowering of standards and the non-applicability of human rights treaties to the State that carries out extraterritorial mass surveillance. On the contrary, the focus of the assessment must shift to

---

ment of 23 February 2016, no. 11138/10, paras 110–111; *M.N. et al. v. Belgium*, judgment of 5 March 2020, no. 3599/18, paras 101–109. Similarly, with regard to digital mass surveillance, ECtHR, *Liberty and Others v. The United Kingdom*, judgment of 1 July 2008, no. 58243/00, paras 64–70.

129 Clearly so, ECtHR, *Al-Skeini* (no. 128), para. 142. See also Tomuschat (n. 125), 100 ff.

130 ECtHR, *Big Brother Watch and Others v. The United Kingdom*, judgment of 13 September 2018, nos 58170/13, 62322/14 and 24960/15, para. 271; *Centrum för Rättvisa v. Sweden*, judgment of 19 June 2018, no. 35252/08, para. 111. In that regard, both chamber judgments were fully confirmed by the Grand Chamber's judgments of 25 May 2021, see ECtHR, *Big Brother Watch and Others v. The United Kingdom* (GC), paras 272, 344, 358; *Centrum för Rättvisa v. Sweden* (GC), para. 258, 272.

131 Federal Constitutional Court, judgment of 19 May 2020, 1 BvR 2835/17, paras 87 ff. – BND.

132 Weiler (n. 125), 659.

133 See Milanović (n. 116), 124; Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung. Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?,' EuZW 27 (2016), 448–454 (450).

the effects of the surveillance.[134] If virtual surveillance produces the same or similar infringements as physical surveillance, both approaches should not be treated differently.[135] The lack of direct physical impairment of the person whose data are intercepted is irrelevant.[136] It is sufficient that an effective accessibility to and control of the online data can be ascertained. No physical influence on the data owner is required.[137] In contrast to those human rights, which aim to protect the physical integrity of a person, such as the right to life and limb, the right to privacy aims to safeguard personal identity, autonomy and self-determination.[138] Finally, the finding that foreigners abroad fall within the object and purpose of human rights law does not produce asymmetries or collisions with the principle of non-intervention. Human rights treaties are grounded in the idea that all human beings possess inherent dignity that deserves protection. Moreover, since only the State authority itself is obliged to respect human rights when taking action beyond its territory, the allegation of an unlawful human rights *octroi* on a foreign State is erroneous.[139] There is simply no interference with the action and the legislative power of any foreign State authority.[140]

---

134 Peter Margulies, '*The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism,*' Fordham L. Rev. 82 (2014), 2137–2167 (2152).

135 Correctly so, Weiler (n. 125), 660.

136 See Ulrich Fastenrath, 'Article 1 ECHR' in: Katharina Pabel and Stefanie Schmahl (eds), *Internationaler Kommentar zur EMRK* (Köln: Wolters Kluwer 2022), Art. 1 para. 106; see also Wolfgang Hoffmann-Riem, 'Freiheitsschutz in den globalen Informationsinfrastrukturen,' JZ 69 (2014), 52–63 (56). Different assessment by Gärditz (n. 118), 476 ff.

137 See Wolfgang Ewer and Tobias Thienel, 'Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals,' NJW 67 (2014), 30–35 (32); Helmut P. Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht,' AVR 52 (2014), 375–406 (392). Different view by Stefan Talmon, 'Der Begriff der 'Hoheitsgewalt'' in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste,' JZ 69 (2014), 783–787 (784).

138 Andreas Fischer-Lescano, 'Der Kampf um die Internetverfassung: Rechtsfragen des Schutzes globaler Kommunikationsstrukturen vor Überwachungsmaßnahmen,' JZ 69 (2014), 965–974 (970). Even metadata do provide detailed information about the intimate life of an individual, see Laura K. Donohue, *The Future of Foreign Intelligence. Privacy and Surveillance in a Digital Age* (Oxford: Oxford University Press 2016), 39 ff.

139 See Gärditz (n. 118), 472; Andreas von Arnauld, 'Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts,' Berichte der Deutschen Gesellschaft für Internationales Recht 47 (2016), 1–34 (12–13); Marko Milanović, *Extraterritorial Application of Human Rights Treaties* (Oxford: Oxford University Press 2011), 118 ff. Different assessment by Sa-

b) Extraterritorial Applicability of Human Rights Treaties to Digital Interferences by Private Third Parties and Non-State Actors

When it comes to cross-border and extraterritorial interventions by private third parties and non-State actors, other considerations must be made. Not every cyber activity by a non-State actor is attributable to a State. On the contrary, private third parties and non-State actors also collect or access data from others for their own (economic) motivation or even unlawful intent, without any State authority being responsible for these actions. For instance, the posting of hateful comments that exceed the threshold of tort law or criminal offenses are in principle excluded from the direct possibility of regulation under international law. Rather, hate speech by private individuals is subject to national tort or penal laws, which must, of course, be compatible with human rights.[141] The same applies to search engine operators, which are growingly confronted with de-referencing requests by individuals that relate to their 'right to be forgotten' enshrined in EU law, even in transnational settings.[142]

In these regards, cross-border situations between private third parties and non-State actors in cyberspace create difficulties. While no State (and, consequently, no international organisation) may claim sovereignty over cyberspace as such, States are empowered to exercise sovereign prerogatives and jurisdiction over any cyber infrastructure on their territory and over activities associated with that cyber infrastructure.[143]

In cross-border situations, however, the exercise of extraterritorial jurisdiction under customary law requires a legitimising genuine link.[144] This link can be based on the principles of subjective or objective terri-

---

mantha Besson, 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to,' LJIL 25 (2012), 857–884 (864 ff.).

140 See Stefanie Schmahl, 'Grundrechtsbindung der deutschen Staatsgewalt im Ausland,' NJW 73 (2020), 2221–2224 (2223).

141 See Stefanie Schmahl, 'Herausforderungen der Regulierung im Cyberspace: Systematisierungsansätze aus der Perspektive des Völkerrechts,' ZÖR 73 (2018), 3–37 (19–20).

142 See, e.g., CJEU, *Google Spain* (n. 62), *Google LLC v. CNIL* (n. 62).

143 Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Cham: Springer 2017), 23; Victoria Ibold, 'Transnational Jurisdiction for Cybercrimes de lege lata and de lege ferenda,' Eu Const. L. Rev. 10 (2020), 255–271 (257), both with further references.

144 Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, Oxford: Oxford University Press 2015), 34 ff. and 79–80.

toriality, which concern the location of where an action is initiated or consummated, as well as on passive or active personality, depending on the nationality of the acting or the affected persons.[145] The courts called for in connection with cross-border online activities usually focus their attention primarily on the author of the unlawful Internet content or the illegal actions as well as on the nexus established by the effects principle, which focuses on the ramifications of an act within a State.[146] This approach to exercising extraterritorial jurisdiction to prescribe and adjudicate Internet disputes is legitimate. If States were unable to regulate extraterritorial actions by private individuals or private corporations, this would amount to surrendering their sovereignty in cyberspace.[147] This is exactly why Article 3 of the EU's General Data Protection Regulation[148] codifies an extensive type of 'territorial scope' built on an effect-based jurisdictional nexus. It aims at protecting the digital privacy of persons in the European Union against the backdrop of the global networked digital era, regardless of the geographical location of a data controller or data processor.[149]

While the States' extraterritorial jurisdiction to prescribe and adjudicate is determined by international law, the jurisdiction to enforce these rules beyond their territorial borders is severely limited.[150] Unless there is an agreement between the States in question, which is largely the case

145 See Uta Kohl, 'Jurisdiction in Cyberspace' in: Tsagourias and Buchan (n. 25), 30–54 (33); Kittichaisaree (n. 143), 24, 27–29. Skeptical assessment by Daniel Bethlehem, 'The End of Geography: The Changing Nature of the International System and the Challenge to International Law,' EJIL 25 (2014), 9–24 (22).

146 See, e.g., ECtHR, *Perrin v. The United Kingdom*, decision of 18 October 2005, no. 5446/03, The Law, B. & C., CJEU, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, judgment of 1 October 2015, case C-230/14, ECLI:EU:C:2015:639, paras 19 ff.; *Google Spain* (n. 62), para. 80; *Google LLC v. CNIL* (n. 62), paras 56–58; *Bolagsupplysningen* (n. 62), paras 42 ff.; *Mittelbayerischer Verlag KG v. SM*, judgment of 17 June 2021, case C-800/19, ECLI:EU:C:2021:489, paras 34 ff. With regard to the case-law of German criminal courts, see Ibold (n. 143), 263–264.

147 Stefanie Schmahl, 'Zwischenstaatliche Kompetenzabgrenzung im Cyberspace,' AVR 47 (2009), 284–327 (305–306). Similar assessment by Ryngaert (n. 144), 81.

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

149 Stephan Koloßa, 'The GDPR's Extra-Territorial Scope. Data Protection in the Context of International Law and Human Rights Law,' HJIL 80 (2020), 701–818 (794–795, 807).

150 Kittichaisaree (n. 143), 26; Kohl (n. 145), 51 ff.; Schmahl (n. 147), 314 ff.

under EU and Council of Europe law,[151] there is no obligation under general international law for States to recognise, tolerate or enforce foreign sovereign acts on their own territory.[152] Enforcement jurisdiction remains almost exclusively territorial.[153] This again shows the particular difficulty of regulatory efforts in cyberspace. Deficits in identification, ambiguities in territorial localisation and areas, in which national tort or criminal law, as well as EU law, cannot be effectively enforced abroad, represent high hurdles in the fight against online crimes or unlawful online interferences. To counter this situation, both the ECtHR[154] and the CJEU[155] have established the principle of provider liability for cross-border online interferences by non-State actors. The liability of the online service provider reacts to the problem of de-territorialisation in cyberspace.[156] Internet platforms are easier to localise and therefore represent a valuable alternative strategy for protecting human rights in the digital sphere.[157] The already mentioned German Network Enforcement Act[158] addresses precisely this point and aims to establish the accountability of these intermediaries.

Similar parameters apply in relation to the automatised reference and information systems by search engine operators and the individual's request of transborder de-referencing based on the 'right to be forgotten' under EU law. It is true that an obligation of the search engine operators to worldwide de-referencing could initiate 'a race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale,'[159]

---

151 For more detail see Ibold (n. 143), 259 ff.

152 See the fundamental essay by Michael Akehurst, 'Jurisdiction in International Law,' BYIL 46 (1972/73), 145–275. More recently, see Alex Mills, 'Rethinking Jurisdiction in International Law,' BYIL 84 (2014), 187–239.

153 Mills (n. 152), 195. See also Schmahl (n. 141), 24–26.

154 ECtHR, *Delfi AS* (n. 112), paras 125 ff., 159; *Magyar Tartalomszolgáltatók Egyesülete* (n. 112), paras 62 and 69.

155 CJEU, *Google Spain* (n. 62), paras 28 ff., 48 ff.; *Tobias McFadden v. Sony Music Entertainment Germany GmbH*, judgment of 15 September 2016, C-484/14, ECLI:EU:C:2016:689, paras 80 ff. Critical assessment by Reto Mantz, 'Rechtssicherheit für WLAN? Die Haftung des WLAN-Betreibers und das McFadden-Urteil des EuGH,' EuZW 27 (2016), 817–820 (819).

156 Cornils (n. 111), 425.

157 See Cornils (n. 111), 423. See also Kersten (n. 86), 202; Eifert (n. 111), 1450–1451.

158 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) of 1 September 2017, Bundesgesetzblatt 2017 I, p. 3352, last modified on 3 June 2021 in: Bundesgesetzblatt 2021 I, 1436.

159 Advocate General Maciej Szunpar, *Google LLC v. CNIL*, opinion of 10 January 2019, case C-507/17, ECLI:EU:C:2019:15, para. 61.

since in particular non-European countries impacted by worldwide de-referencing could, in response, also implement worldwide de-referencing under their domestic laws.[160] Therefore, the CJEU is right in founding that the 'right to be forgotten' as recognised under EU law does not indispensably require search engine operators to comply with de-referencing requests on all the versions of their search engines that exist worldwide.[161] Or in other words, there is currently no obligation to introduce an extraterritorial scope on the operation of the 'right to be forgotten.' However, at the same time, the Court emphasises that EU law does not prohibit such a practice, by drawing attention to the EU Parliament's and the EU Member States' ability to extend the rights to privacy and the protection of personal data extraterritorially.[162] This approach is also reinforced by the CJEU's *GC, AF, BH, ED v. CNIL* decision, where the Court extended the grounds upon which EU citizens can request search engine operators to de-reference search results, specifically where such results contain sensitive personal information relating to, *inter alia*, ethnic origin, political opinions, religious beliefs, and sexual orientation.[163]

6. *Discrimination Issues in the Virtual World Through Algorithms*

Algorithms, predictive analytics and data-based differentiation decisions represent a sixth challenge for the implementation of international human rights. Algorithms are not only used in Internet search portals, but increasingly also in the business world, in legal technology, in social security systems, in administrative procedures and in the area of predictive policing.[164] The distinctions made by algorithms are based on programmed

160 Zalnieriute (n. 62), 263.
161 CJEU, *Google LLC v. CNIL* (n. 62), paras 66–71.
162 CJEU, *Google LLC v. CNIL* (n. 62), paras 73–75. See also Zalnieriute (n. 62), 266.
163 CJEU, *GC, AF, BH, ED v. CNIL*, judgment of 24 September 2019, case C-136/17, ECLI:EU:C:2019:773, paras 17 and 68–69.
164 For an overview of the various constellations, see, e.g., Mario Martini and David Nink, 'Wenn Maschinen entscheiden... vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz,' NVwZ 36 (2017), 681–682; Thomas Söbbing, *Fundamentale Rechtsfragen Künstlicher Intelligenz* (Frankfurt am Main: Deutscher Fachverlag 2019), 6 ff.; Carsten Orwat, *Diskriminierungsrisiken durch Verwendung von Algorithmen* (Baden-Baden: Nomos 2019), 17 ff.; Carmen Freyler, 'Robot-Recruiting, Künstliche Intelligenz und das Antidiskriminierungsrecht,' NZA 37 (2020), 284–290 (285); Ines Härtel, 'Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren,' LKV 29 (2019),

and aggregated parameters and metrics, which in turn result from analyses of personal data from various groups of people.[165] The result of the parameters obtained resembles the application of stereotypes and increases the risk that people are no longer perceived as individuals and in their subject quality, but are only treated in a standardised manner as part of a group. Such a phenomenon affects not only the individual, but also the principles of equality and non-discrimination.[166] It is undisputed that the use of algorithms can reinforce structural inequality and power asymmetries.[167] Moreover, recent developments in some countries give cause for concern that the combination of artificial intelligence with big data might strengthen the surveillance mechanisms of States and non-State actors.[168] One example is the expanded surveillance by the Chinese Government, which uses artificial intelligence and algorithms to access biodata and DNA databases, particularly to monitor ethnic minorities.[169]

Against this background, the question must be answered how it can be ensured that the use of algorithms does not become a new form of discrimination that the prohibitions on discrimination enshrined in human rights treaties can no longer adequately cope with. Although a dynamic interpretation of the human rights prohibitions on discrimination remains fundamentally possible, the formation of individual comparison parameters, which are essential for handling prohibitions of discrimination, is challenging with artificially programmed algorithms. These are typically geared towards mathematical, leeway-free group fairness, and

---

49–50 (54 ff.); Renate Schaub, 'Verantwortlichkeit für Algorithmen im Internet,' Zeitschrift für Innovations- und Technikrecht 2019, 2–7; Raphael Koch and Christine Biggen, 'Der Einsatz Künstlicher Intelligenz zur Organisation and proaktiven Überprüfung von Onlinebewertungen,' NJW 73 (2020), 2921–2925.

165 For more detail see Orwat (n. 164), 3 ff. See also Thomas Wischmeyer, 'Regulierung intelligenter Systeme,' AöR 143 (2018), 1–66 (14).

166 See, e.g., Christian Ernst, 'Algorithmische Entscheidungsfindung und personenbezogene Daten,' JZ 72 (2017), 1026–1036 (1032 ff.); Mario Martini, 'Algorithmen als Herausforderung für die Rechtsordnung,' JZ 72 (2017), 1017–1025 (1018); Orwat (n. 164), 24 ff.; Philipp Hacker, 'Teaching Fairness to Artificial Intelligence,' CMLRev. 55 (2018), 1143-1186 (1145 ff.).

167 See Wischmeyer (n. 165), 26; Freyler (n. 164), 285; Hans Steege, 'Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz,' Multimedia und Recht 2019, 715–721 (716 ff.).

168 Kriebitz and Lütge (n. 63), 102.

169 See Uyghur Human Rights Project, 'China's Repression and Internment of Uyghurs: U.S. Policy Responses,' House Committee on Foreign Affairs: Subcommittee on Asia and the Pacific (26 September 2018).

not on individual justice.[170] This difficulty is particularly evident when a fully automated computer programme makes the decision, and neither the programmer nor the user can explain or reliably predict the result of the decision-making process. In these cases, machine algorithms function as black boxes.[171]

One of the most important regulations to protect against algorithmic discrimination risks is the prohibition of automated decisions in data protection law. According to Article 22 (1) of the EU's General Data Protection Regulation,[172] the individual concerned has the right not to be subject to a decision based solely on automated processing that has a legal effect on him or her or significantly affects him or her in a similar way. The General Data Protection Regulation does not fully specify what types of automated decisions are meant. However, it is certain that no content-related assessment can be made solely on the basis of algorithm-created decisions without a natural person having the final decision-making authority.[173] Simultaneously, it must also be taken into account that it will be difficult for the human decision-maker to completely free him- or herself from the automated preliminary decision by the algorithms. It is much more likely that the human decision-maker will only perform a plausibility check based on the result found by the algorithms.

Modern behavioural sciences have revealed that algorithms, as a rule, work as nudges and have a strong manipulation potential.[174] Thus, there remains the risk that even the prescribed control of the result based on al-

170 Jon Kleinberg et al., 'Discrimination in the Age of Algorithms,' Journal of Legal Analysis 10 (2018), 113–174 (161 ff.).

171 For a fuller account see Frank Pasquale, *The Black Box Society. The Secrect Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press 2015). *Cf.* also David Roth-Isigkeit, 'Staatshaftungsrechtliche Aspekte des Einsatzes automatisierter Entscheidungssysteme in der öffentlichen Verwaltung,' AöR 145 (2020), 321–351 (335). Different assessment by Yoan Hermstrüwer, 'Fairnessprinzipien in der algorithmischen Verwaltung,' AöR 145 (2020), 479–521 (492 ff.).

172 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and repealing Directive 95/46/EC, OJ 2016 L 119/1–88.

173 See Mario Martini, 'Article 22' in: Boris P. Paal and Daniel A. Pauly (eds), *Datenschutz-Grundverordnung/Bundesdatenschutzgesetz* (2nd edn, München: C.H. Beck 2018), para. 29.

174 See Laurence O'Hara, 'Grundrechtsschutz vor psychisch vermittelter Steuerung,' AöR 145 (2020), 133–187 (162–165); Sophie V. Knebel, *Die Drittwirkung der Grundrechte und -freiheiten gegenüber Privaten. Regulierungsmöglichkeiten sozialer Netzwerke* (Baden-Baden: Nomos 2018), 106 ff.

gorithms by a natural person will prove to be practically ineffective.[175] The States, in particular the Member States of the European Union, are therefore obliged to put in place a legal system that addresses these problems of bounded autonomy under a human rights perspective.[176] On the one hand, the programming of algorithms and self-learning intelligent systems must be carried out transparently, in accordance with the principle of non-discrimination.[177] The technological and socio-technical design of each automated decision-making system must further be performed in a way that corresponds to the rights, freedoms and legitimate interests of the data subjects. This requires a full assessment and balancing of the positive and negative impacts of automated decision-making.[178] On the other hand, it must be ensured that legal remedies are at hand that can effectively repeal any alleged unlawful discrimination by artificial intelligence systems.[179]

7. Cyborgs and Humanoid Robots as New Rights-Holders or New Duty-Bearers?

Finally, it is to be expected that the further development of technology can bring about fundamental changes in human rights protection in the medium or long term. To put it briefly: Will digitalisation, especially the development of artificial intelligence, lead to a new or additional form of rights-holders or duty-bearers? The creation of cyborgs and human-like machines seems to be within reach due to the evolvement of robotics. The 'artificial human being' does not necessarily have to be a physical artifact but can also be disembodied, for example, by simulating his or her

175 Wolfgang Hoffmann-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht,' AöR 142 (2017), 1–42 (36).

176 See Orwat (n. 164), 105 ff.; McGregor, Murray and Ng (n. 66), 337. See also Wibke Werner, 'Schutz durch das Grundgesetz im Zeitalter der Digitalisierung,' Neue Juristische Online-Zeitschrift 2019, 1041–1046 (1043).

177 Unanimous view, see, e.g., Martini (n. 166), 1022; Schaub (n. 164), 7; Freyler (n. 164), 290; McGregor, Murray and Ng (n. 66), 335 ff.; Kriebitz and Lütge (n. 63), 99; Kühling (n. 73), 535 ff.

178 For more detail, see Christian Djeffal, 'The Normative Potential of the European Rule on Automated Decisions: A New Reading for Art. 22 GDPR,' HJIL 80 (2020), 847–879 (857 ff.).

179 Werner (n. 176), 1043; Susanne Beck, 'Diskriminierung durch Künstliche Intelligenz?,' ZRP 52 (2019), 185 (185). For more detail, see Ljupcho Grozdanovski, 'In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law,' CMLRev. 58 (2021), 99-136 (120 ff.).

behaviour through a digital representation.[180] Is such a virtual person or humanoid robot suitable as a holder or as a duty-bearer of human rights? What are the limits of the dynamic interpretation of human rights treaties when human life (also) takes place virtually? In trying to answer these questions, it is important to make clear distinctions from the outset.

Firstly, it is to be noted that the recognition of the legal personality of new virtual or humanoid entities does not automatically entail that these entities enjoy human rights or that they are committed to respect or protect the human rights of others.[181] But experience shows that the ascription of legal personality and autonomy has often been linked to the ability to act which is secured with certain substantial human rights (such as freedoms of communication, business and property) and procedural rights. For instance, under Article 19(3) of the German Basic Law, the fundamental rights of the Basic Law shall also apply to domestic legal persons to the extent that the nature of such rights permits. The Federal Constitutional Court recognises the entitlement to enjoy basic rights not only for domestic legal persons but also for mixed-business companies,[182] legal persons based in an EU Member State,[183] and legal persons governed by private law, which are operated domestically for profit and entirely owned by a Member State of the EU.[184] In view of globalisation and digitalisation, legal scholars are even campaigning for a dynamic extension of the scope of Article 19(3) of the Basic Law to include companies that are based outside of Europe but are active in Germany.[185] This idea applies above all to global digital platforms, but it could also be transferred to artificial intelligence and humanoid robots.

Secondly, a distinction must be made between the types of artificial intelligence. So far, there has been no need to qualify cyborgs as a separate category of human rights-holders. The name 'cyborg' is an acronym

180 Christian L. Geminn, 'Menschenwürde und menschenähnliche Maschinen und Systeme,' DÖV 73 (2020), 172–181 (173).

181 As to the concepts of rights, laws, human rights, and critiques of rights see, e.g., Anne Peters, 'The Importance of Having Rights,' HJIL 81 (2021), 7–22, with further references.

182 Federal Constitutional Court, judgment of 22 February 2011, 1 BvR 699/06, BVerfGE 128, 226 – Fraport.

183 Federal Constitutional Court, decision of 19 July 2011, 1 BvR 1916/09, BVerfGE 129, 78 – Cassina.

184 Federal Constitutional Court, judgment of 6 December 2016, 1 BvR 2821/11, BVerfGE 143, 246 – Vattenfall.

185 See Ralf Müller-Terpitz, 'Die Grundrechtsberechtigung juristischer Personen im Zeitalter der Globalisierung und Digitalisierung,' JZ 75 (2020), 1080–1087.

derived from 'cybernetic organism.'[186] In medicine, the use of complex internal technology is no longer uncommon. According to a narrow interpretation, cyborgs are humans with technical implants such as cardiac pacemakers, complex prostheses and cochlea or retina implants.[187] There is no doubt that human beings with such in-body technology will continue to enjoy human rights to the same extent as individuals without such implants.[188]

However, the legal situation is more difficult when a person's brain is controlled by implants, for example, through brain stimulation. With the help of a stereotactic operation, electrodes are placed minimally invasively on the patient at a certain point in the brain, which is previously determined by a magnetic resonance and computer tomographic image of the brain.[189] For the time being, the devices have been used in particular for motoric problems suffered by Parkinson's patients.[190] Nevertheless, there are first insights into the possibility of influencing states of mind (which so far have mainly occurred as side effects) to increase memory performance and other cognitive abilities.[191] At this point, besides major ethical issues, the question arises as to whether a person with a brain implant, i.e. a cyborg in a wider sense, could be regarded as a new category of a holder of fundamental rights. In any case, such cyborgs constitute a tense combination of human and artificial intelligence.[192] If the artificial intelligence can be controlled from the outside, which is usually the case via computers with deep learning mechanisms, this entails considerable

186 Ronald Kline, 'Where are the Cyborgs in Cybernetics?,' Social Studies of Science 39 (2009), 331–362 (331).

187 Katherine Hayles, 'The Life Cycle of Cyborgs: Writing the Posthuman' in: Chris Hables Gray (ed.), *The Cyborg Handbook* (London: Routledge 1995), 321–340 (322–335).

188 See Karin Harasser, *Körper 2.0: Über die technische Erweiterbarkeit des Menschen* (Bielefeld: Transcript Verlag 2013), 9 ff.; Jens Kersten, 'Mensch und Maschinen,' JZ 70 (2015), 1–8 (4–5).

189 Söbbing (n. 164), 55–56.

190 See Schliesky (n. 78), 699.

191 See Dominik Groß, 'Neuro-Enhancement unter besonderer Berücksichtigung neurobionischer Maßnahmen' in: Albrecht Wienke et al. (eds), *Die Verbesserung des Menschen: Tatsächliche und rechtliche Aspekte der wunscherfüllenden Medizin* (Berlin/Heidelberg: Springer 2009), 85–118 (90 ff.); Christoph Kehl and Christopher Coenen, *Technologien und Visionen der Mensch-Maschine-Entgrenzung, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)*, Arbeitsbericht Nr. 167 (Berlin, 2016), 82; Schliesky (n. 78), 699.

192 Söbbing (n. 164), 56–57.

risks for the human being concerned and others.[193] Such cyborgs are not entirely free in the legal sense and can therefore hardly be regarded as autonomous acting persons and be held responsible for their actions without taking into account the work of the manufacturer or the implanter of the artificial components.[194]

Similar considerations already apply to other preliminary stages of the 'virtual human being,' for example, to systems that can receive voice commands and conduct conversations, such as the Twitter bot named 'Tay.'[195] Such voice-controlled systems are in a sense human-like and influence or even replace the decision-making power of real people, similar to self-driving cars and unmanned aircraft systems.[196] In such situations, it is no longer clear who actually could be regarded as the holder of human rights – the human cyborg, the computerised brain stimulator, the programmer, or all together? The established human rights system reaches its limits when the attribution criteria become blurred. In any case, the question of when human existence begins and when it ends will have to be posed much more sharply in this context than ever before.

Last but not least, it is particularly challenging for the human rights system when one looks at the humanoid robots, i.e. machines which are built on deep self-learning in order to mimic human cognitive functions.[197] In 2017, Saudi Arabia granted 'citizenship' to a humanoid robot named Sophia.[198] This symbolic action has been described in the media as a cynical act for a country that denies girls and women equal rights.[199] Nonetheless, the episode is significant because it was the first time that a State purported to give a kind of legal personality to a robot or artificial

193 See Eric Hilgendorf, 'Menschenwürde und Neuromodulation' in: Jan C. Joerden, Eric Hilgendorf and Felix Thiele (eds), *Menschenwürde und Medizin* (Berlin: Duncker & Humblot 2013), 865–874 (867 ff.).

194 Söbbing (n. 164), 63 ff. See also Jochen Hanisch, 'Zivilrechtliche Haftungskonzepte für Robotik' in: Eric Hilgendorf (ed.), *Robotik im Kontext zwischen Recht und Moral* (Baden-Baden: Nomos 2014), 27–63 (38).

195 Wischmeyer (n. 165), 10 ff. See also Kriebitz and Lütge (n. 63), 98.

196 See, e.g., Söbbing (n. 164), 49–50, 67 ff.; Kersten (n. 188), 2.

197 For more detail see Themis Tzimas, 'Artificial Intelligence and Human Rights: Their Role in the Evolution of AI,' HJIL 80 (2020), 533–557 (544 ff.).

198 See the website of Hanson Robotics, Sophia (available at: https://www.hansonrobotics.com/sophia/).

199 See Cleve R. Wootson Jr., 'Saudi Arabia Which Denies Women Equal Rights, Makes Robot a Citizen,' Washington Post (29 October 2017).

intelligence entity.[200] A related possibility is that a human's personality or consciousness might be uploaded and stored on a computer or a network. Some scientists are already working on this idea.[201] Although these are isolated cases and the worldwide existence of human-like robots is part of science fiction (albeit probably not too far away), human rights doctrine is called upon to deal with this phenomenon at an early stage. Can or should humanoid robots enjoy legal personality and human rights? Or should they, in reverse, be considered as duty-bearers of human rights?

The first (human) reaction to the question of the enjoyment of human rights by humanoid robots is certainly negative, since the theoretical foundation for human rights is to be seen in the dignity of the human being, which includes personal autonomy and vulnerability.[202] On the other hand, it should be borne in mind that States and private companies are also artificial legal products, i.e., collective fictions of legal personhood.[203] In particular, private companies are endowed with a wide range of basic (human) rights, such as the right to a fair trial or the right to property.[204] A comparison with the legal status of animals also shows that animal rights have varied considerably over time.[205] In recent times, legal debate even growingly focuses on the judicial recognition of nature as a subject of rights.[206] Legal subjectivity has always been and still is relative. Legal systems are free to recognise non-human legal subjects and to define their

200 Jacob Turner, *Robot Rules. Regulating Artificial Intelligence* (London: Palgrave Macmillan 2019), 173.

201 See Geminn (n. 180), 173.

202 Similarly, Peters (n. 181), 10–11.

203 See Jan-Erik Schirmer, 'Rechtsfähige Roboter?,' JZ 71 (2016), 660–666 (662). See also Visa A J Kurki, 'Why Things Can Hold Rights: 'Reconceptualizing the Legal Person'' in: Visa A J Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Cham: Springer 2017), 69–89 (82 ff.).

204 See the Federal Constitutional Court judgments of 22 February 2011, 19 July 2011, and 6 December 2016, cited in n. 182–184.

205 For a fuller account see Rafal Michalczak, 'Animals' Race Against the Machines' in: Kurki and Pietrzykowski (n. 203), 91–101 (94 ff.); Ryan Abbott, *The Reasonable Robot. Artificial Intelligence and the Law* (Cambridge: Cambridge University Press 2020), 23; Jens Kersten, *Das Anthropozän-Konzept* (Baden-Baden: Nomos 2014), 88 ff.

206 See, e.g., Marjorie Andrea González Ramírez, 'The Judicial Recognition of Nature as a Subject of Rights: An Answer to Tackle Environmental Problems in Colombia and to Broaden the Community that is Granted Justice,' Die Friedens-Warte 93 (2020), 148–172 (149 ff.), with further references.

legal status and their rights.[207] This does not mean that animals, private companies, legal persons or artificial intelligence should have the same rights as human beings. For example, human-centric rights that are anchored in social relationships such as dignity or privacy will not be suitable for artificial intelligence.[208] However, tiered ownership of fundamental rights does not seem to be excluded from the outset.[209] Some scholars call for the development of a new category of the legal subject, halfway between person and object.[210]

Legal personality, rights and duties for artificial intelligence and humanoid robots are no longer just a matter for a purely academic debate.[211] In 2017, the European Parliament passed a resolution containing recommendations on Civil Law Rules on Robotics.[212] The European Parliament suggested, *inter alia*, to create a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for compensating any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact independently with third parties. Thereby, the European Parliament left open the question of whether artificial intelligence could be housed within

207 See Jens Kersten, 'Relative Rechtssubjektivität. Über autonome Automaten und emergente Schwärme,' Zeitschrift für Rechtssoziologie 37 (2017), 8–25 (9–10). Similarly, with regard to animals' rights: Anne Peters, 'Liberté, Égalité, Animalité: Human-Animal Comparisons in Law,' Transnational Environmental Law 5 (2016), 25–53 (46 ff.).

208 Geminn (n. 180), 175.

209 As far as can be seen, this is a uniform view, see Kersten (n. 188), 7–8; Schirmer (n. 203), 662 ff.; Susanne Beck, 'Sinn und Unsinn von Statusfragen' in: Eric Hilgendorf and Jan-Philipp Günther (eds), *Robotik und Gesetzgebung* (Baden-Baden: Nomos 2013), 239–260 (255 ff.); Andreas Fischer-Lescano, 'Natur als Rechtsperson,' Zeitschrift für Umweltrecht 29 (2018), 205–216 (213–214); Gerhard Wagner, 'Roboter als Haftungssubjekte? Konturen eines Haftungsrechts für autonome Systeme' in: Florian Faust and Hans-Bernd Schäfer (eds), *Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz* (Tübingen: Mohr Siebeck 2019), 1–39 (29).

210 See, Ryan Calo, 'Robotics and the Lessons of Cyberlaw,' Cal. L. Rev. 103 (2015), 513–563 (549); Jack B. Balkin, 'The Path of Robotics Law,' Cal. L. Rev. Circuit 6 (2015), 45–60 (57).

211 Rightly so, Turner (n. 200), 174.

212 European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2005/2103(INL), para. 59.

recognised legal categories of personality or whether new ones, with their own specific features and implications, would be needed.[213]

In any case, granting a humanoid robot legal personality could be a valuable firewall between existing humans and legal persons and the harm and injuries which artificial intelligence could cause.[214] The rights, duties and liabilities of a company are usually separate from those of its owners or controllers. A company's creditors can only recourse to that company's own assets, a feature known as 'limited liability.' The limited liability of companies is a powerful tool in protecting human beings from risk and thereby encouraging innovation.[215] Arguably, the justifications for providing such legal personality to artificial intelligence are even stronger than for protecting human owners from the liability of companies. Humanoid robots can do something that existing companies cannot do: make autonomous decisions without human input.[216] Whereas a company is merely a collective fiction for human volitions, artificial intelligence by its nature has its own independent 'consciousness' or 'will,' which functionally determines for itself in an autonomous manner how a given task is to be performed.[217]

Yet, as important as these concepts are, they all go beyond the anthropocentric character of human rights treaties.[218] Existing legal systems, both

213 See Melinda F. Lohmann, 'Ein europäisches Roboterrecht – überfällig oder überflüssig?,' ZRP 51 (2018), 168–171; Horst Eidenmüller, 'The Rise of Robots and the Law of Humans,' Zeitschrift für Europäisches Privatrecht 25 (2017), 765–777; Renate Schaub, 'Interaktion von Mensch und Maschine,' JZ 72 (2017), 342–349 (346).

214 Turner (n. 200), 187. See also Gunther Teubner, 'Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteursstatus in Recht und Politik,' Zeitschrift für Rechtssoziologie 27 (2006), 5–30 (30); *id.*, 'Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten,' AcP 218 (2018), 155–205 (162).

215 Rightly so, Turner (n. 200), 187.

216 Tzimas (n. 197), 546 ff.; Turner (n. 200), 187.

217 See Gunther Teubner, 'Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law,' Max Weber Lecture Series No. 2007/04 (available at: http://hdl.handle.net/1814/6960), 1–21 (10 ff.). See also Turner (n. 200), 187; Abbott (n. 205), 34.

218 Similarly, Claus Müller-Hengstenberg and Stefan Kirn, 'Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems?,' Multimedia und Recht 2014, 307–313 (308); Jan-Erik Schirmer, 'Von Mäusen, Menschen und Maschinen – Autonome Systeme in der Architektur der Rechtsfähigkeit,' JZ 74 (2019), 711–718 (716). Different assessment by Fischer-Lescano (n. 209), 214–216; Kersten (n. 207), 22.

international and national, are fundamentally human-centred in the sense that they take for granted that humans are the most developed form of being and that the welfare of humans constitutes the ultimate goal of morals and laws.[219] Even a dynamic interpretation of human rights treaties in order to include humanoid robots at least partially as autonomous actors, responsible entities, duty-bearers, and rights-holders will be impossible. The Expert Group on Liability and New Technologies, set up by the European Commission in response to the European Parliament's 2017 proposal, explicitly stresses that it is neither necessary nor sensible to give legal personality to autonomous systems. Rather, the harm these systems may cause should be attributable to existing persons or bodies.[220] The digital agenda of the European Union of 19 February 2020, which consists of a European strategy for data, a report on the safety and liability implications of artificial intelligence, the Internet of things and robotics, and a white paper on artificial intelligence, fully supports this assessment.[221] The same holds true for the Commission's legislative initiative of 21 April 2021 to harmonise rules on artificial intelligence.[222] These views are also largely consistent with international artificial intelligence ethics codes that aim at active cooperation between States to progress responsible stewardship of trustworthy artificial intelligence.[223]

A similar observation can be found in the ECtHR's case-law on animal rights. In 2008, Austrian animal activists invoked the existence of an animal right to free movement in order to enforce judicially the release of

219 Tzimas (n. 197), 553.

220 See Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (European Union, 2019), 37 ff.

221 European Commission, COM (2020) 66 final; COM (2020) 64 final; COM (2020) 65 final. For more detail, see Philipp Hacker, 'Europäische und nationale Regulierung von Künstlicher Intelligenz,' NJW 73 (2020), 2142–2147 (2142 ff.); Stefan Heiss, 'Europäische Haftungsregeln für Künstliche Intelligenz,' EuZW 32 (2021), 932-938.

222 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,' COM (2021) 206 final. Further see Andreas Ebert and Indra Spiecker gen. Döhmann, 'Der Kommissionsentwurf für eine KI-Verordnung der EU,' NVwZ 40 (2021), 1188-1193; Hannah van Kolfschooten, 'EU Regulation of Artificial Intelligence: Challenge for Patients' Rights,' CMLRev. 59 (2022), 81-112 (91 ff.).

223 See, e.g., the Recommendation of the OECD Council on Artificial Intelligence of 22 May 2019, reprinted in ILM 59 (2020), 30 ff. For more detail see Karen Yeung, 'Introductory Note to Recommendation of the Council on Artificial Intelligence (OECD),' ILM 59 (2020), 27–29; Kriebitz and Lütge (n. 63), 85–86.

great apes from confinement and zoos before the ECtHR. However, their complaints were rightly rejected on the grounds of incompatibility *ratione materiae*.[224] This decision shows that no existing human rights treaty can be interpreted so extensively and dynamically in relation to the holders of rights without at the same time contradicting its underlying assumptions and objectives. For this reason, humanoid robots cannot be included as (partial) rights-holders in the international human rights system.[225] It is true that the animal rights discourse aims at recognizing animals as sentient beings in law and as possible bearers of rights, while the current debate about humanoid robots focuses more on liability and obligations, and less on rights. The rationale for granting legal personhood is thus a different one. However, parallels exist in that both animals and humanoid robots do not fit within the human rights scheme; they cannot be considered either as holders or as duty-bearers of human rights.

If one wants to change this legal situation, new treaties would have to be concluded specifically dealing with the legal personhood of artificial intelligence and its ability to exercise rights and duties. But fortunately, this is still part of science fiction, as the influence of humanity is unlikely to be significant in that regard, once artificial, autonomous entities have emerged that surpass human intelligence in many or all aspects. Such an artificial intelligence is rather expected to choose and implement its own goals in a post-human legal or otherwise construed system.[226] In any case, one (dystopian) assumption seems irrefutable: the human focus of the existing legal systems can hardly be preserved after the emergence of artificial entities with an intelligence that is equal or superior to that of humans.[227]

III. Outlook

As always, modern technology is both a blessing and a curse. In general, digitalisation does not require a fundamental paradigm shift but a change of perspective in the normative interpretation of human rights treaties. Many questions can be solved by way of a dynamic interpretation.

---

224 See ECtHR, *Balluch v. Austria*, decision of 25 September 2012, no. 4471/06, paras 23 ff. See also *Stibbe v. Austria*, appl. no. 26188/08, lodged 6 May 2008.

225 Similarly, Tzimas (n. 197), 554; Wagner (n. 209), 30. Differently, Fischer-Lescano (n. 209), 215–216.

226 Geminn (n. 180), 174. Similarly, Teubner, AcP (n. 214), 200.

227 Rightly so, Tzimas (n. 197), 554–555.

However, despite the changed social and technological context due to digitalisation, the decisive factor in any dynamic interpretation of human rights must remain that freedom and responsibility remain two sides of the same coin, both in the analogue and the digital world. The organs of the Council of Europe have rightly expressed this demand in several resolutions.[228] In order to ensure that the negative symptoms of digitalisation do not evoke irreversible social upheaval, ultimately, the State has to prove itself as a guarantor for the protection of the right to privacy and self-determination against anonymous or veiled online attacks and autonomously operating software systems.[229]

In that regard, not everything that appears economically and technologically attractive and enforceable is compatible with the human-centred character of human rights treaties. At least, human-like robots, should they come to 'life' one day, will transform the social and human-centred character of the existing legal systems, both internationally and nationally. Even the current discussion-oriented project for a 'Charter of Digital Fundamental Rights of the European Union,'[230] which in principle deserves support, will not be able to stop such ground-breaking changes.[231] In a post-human era under the aegis of humanoid robots, the protection of human rights will necessarily have to enter a fundamentally new phase. Even more: The challenges which come along with humanoid robots cannot be coped with or solved in a human rights language. This would simply be an overload, which would put the very concept of human rights at fundamental risk.

228 See, e.g., Council of Europe, Report on Technological Convergence, Artificial Intelligence and Human Rights, Doc. 14288 (Recommendation 2102), 10 April 2017, with further references.

229 See Schmidt-Jortzig (n. 116), 13.

230 See https://digitalcharta.eu/.

231 For more detail see Albert Ingold, 'Der Entwurf für eine "Charta der Digitalen Grundrechte der Europäischen Union": Vorhaben, Vorstellungen, Vorbehalte,' Zeitschrift für Gesetzgebung 2018, 193–209; Friedrich Graf von Westphalen, 'Digitale Charta – Erweiterung der europäischen Grundrechte für das digitale Zeitalter,' BB 2018, 899–907. Overly critical assessment by Sebastian J. Golla, 'In Würde vor Ampel und Algorithmus,' DÖV 72 (2019), 673–681 (677 ff.).