Report of Austria to the Council of Europe following Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom.

In line with the Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to Member States on Internet freedom, especially its article 7, Austria presents the attached evaluation to the Council of Europe.

The evaluation was commissioned by the Federal Chancellery of Austria and undertaken by two independent experts, Prof. Berka and Prof. Trappel, both professors at the University of Salzburg. They concluded their study in December 2017, after conducting interviews with all stakeholders from the private sector, civil society, academia and the technical community. Subsequently, the evaluation, originally written in German language, was translated into English; this is the version presented to the Council of Europe.

In addition to this paper it should be noted that the draft of an amendment to the code of criminal procedure (§ 135a StPO; mentioned on page 47 and in footnote 97) was recently adopted and published in the Federal Law Gazette (BGBl. I Nr. 27/2018). In contrast, the 'quick-freeze procedure' (draft sec. 99 para. 1a to 1f TKG 2003, mentioned on pages 47/48 and in footnote 98) has not been adopted by the Federal Parliament.

INTERNET FREEDOM IN AUSTRIA

A SURVEY BASED ON THE RECOMMENDATION CM/REC(2016)5 OF THE COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE TO THE MEMBER STATES REGARDING INTERNET FREEDOM

Authors:
O. Univ. Prof. em. Dr Walter Berka
Univ. Prof. Dr Josef Trappel

Faculty of Public Law/Constitutional and Administrative Law
Department of Communication Studies
of the University of Salzburg

January 2018

Contents

A. INTRODUCTION: NOTION AND CONCEPT OF INTERNET FREEDOM AS PER RECOMMENDATION CM/REC(2016)5 AND THE ANNEX TO THIS REPORT 5

B. INTERNET FREEDOM IN AUSTRIA: GENERAL LEGAL FRAMEWORK AND STANDARDS 6

I. THE CONSTITUTIONAL AND EUROPEAN-LAW FRAMEWORK 7

1. INTERNET FREEDOM AND THE HUMAN-RIGHTS GUARANTEES OF THE ECHR 7

2. THE EUROPEAN LEGAL FRAMEWORK FOR INTERNET FREEDOM 11

3. GENERAL FRAMEWORK FOR THE REGULATION OF INTERNET COMMUNICATION 12

4. LEGISLATION WITH RESPECT TO INTERNET FREEDOM 13

II. FREEDOM OF ACCESS TO THE INTERNET AND THE PROTECTION OF FREE SPEECH AND FFREEDOM OF THE MEDIA ON THE INTERNET 14

1. FREEDOM OF ACCESS 14

2. THE REGULATION OF ONLINE MEDIA 16

3. INTERNET PLATFORMS AND INTERMEDIARY INTERNET SERVICES 19

4. JOURNALISTIC FREEDOM AND INDEPENDENCE IN ONLINE MEDIA 21

5. CONTENT RESTRICTIONS IN INTERNET COMMUNICATION AND ONLINE MEDIA 25

6. IMPLEMENTATION OF THE NET NEUTRALITY PRINCIPLE 32

7. BLOCKING INTERNET ACCESS AND DELETING CONTENT FROM THE INTERNET 33

III. THE FREEDOMS OF ASSOCIATION AND ASSEMBLY AND THE INTERNET 35

1. THE PROTECTION OF THE FREEDOMS OF ASSOCIATION AND ASSEMBLY WITH REGARD TO THE INTERNET 35

2. RESTRICTIONS OF THE FREEDOMS OF ASSOCIATION AND ASSEMBLY 36

IV. THE RIGHT TO RESPECT OF ONE'S PRIVACY AND FAMILY LIFE AND OF DATA PROTECTION ON THE INTERNET 37

1. PROTECTION OF PRIVACY WITH ONLINE MEDIA 37

2. DATA PROTECTION AND THE INTERNET 40

3. PROTECTION OF ANONYMITY ON THE INTERNET AND THE USE OF ENCRYPTION TECHNOLOGIES 42

V. GOVERNMENT SURVEILLANCE OF THE INTERNET 43

1. GENERAL LEGAL CONDITIONS 43

2. OVERVIEW OF THE SURVEILLANCE POWERS OF POLICE AND JUDICIAL AUTHORITIES 44

3. REGARDING SCRUTINY OF SURVEILLANCE POWERS 48

VI. LEGAL REMEDIES 52

C. COMMUNICATION STUDIES ANALYSIS 55

I. FREEDOM OF ACCESS ON THE INTERNET 56

1. INTRODUCTION 56

1.1 FREEDOM OF INFORMATION 57

1.2 THE RESPONSIBILITY AND LIABILITY OF INTERMEDIARIES AND ISPS 58

1.3 INTELLECTUAL PROPERTY AND COPYRIGHTS 59

1.4 FILTER BUBBLES AND ALGORITHMS 59

1.5 NET NEUTRALITY 61

1.6 CYBER-ATTACKS 62

2. THE RESULTS OF THE EXPERT SURVEY 62

2.1 LEGAL FRAMEWORK 62

2.2 CASE LAW 64

2.3 PROSECUTION 65

2.4 ASSESSMENT OF ONLINE CONTENT BY PRIVATE OPERATORS 66

2.5 ACCESS RESTRICTIONS DUE TO COPYRIGHTS AND PATENTS 67

2.6 FILTER BUBBLES AND ALGORITHMS 69

2.7 NET NEUTRALITY 70

2.8 CYBER-ATTACKS 71

3. CONCLUSION 71

II. FREEDOM OF EXPRESSION ON THE INTERNET AND REGULATION OF ONLINE MEDIA 73
1. INTRODUCTION 73
1.1 CHANGES IN JOURNALISM 75
1.2 HATE SPEECH 75
1.3 FAKE NEWS AND DISINFORMATION 77
2. THE RESULTS OF THE EXPERT SURVEY 78
2.1 FREEDOM OF THE MEDIA 78
2.2 JOURNALISM 79
2.3 HATE SPEECH AND FAKE NEWS 79
3. CONCLUSION 81
III. DATA PROTECTION AND THE PROTECTION OF THE PRIVATE SPHERE 82
1. INTRODUCTION 82
1.1 THE STATE 83
1.2 COMPANIES 84
1.3 THE INDIVIDUAL 85
2. THE RESULTS OF THE EXPERT SURVEY 86
2.1 SMARTPHONES 86
2.2 CLOUD APPLICATIONS 86
2.3 ALGORITHM-SUPPORTED BIG-DATA ANALYSES 88
2.4 DEEP PACKET INSPECTION 90
2.5 TROJAN HORSES 90
2.6 DATA PROTECTION IN COMPANIES 91
2.7 CYBER-ATTACKS ON COMPANIES 92
2.8 PUBLIC DATA AT PRIVATE COMPANIES 93
2.9 CYBER-ATTACKS ON PUBLIC DATA 94
2.10 DATA-PROTECTION AWARENESS 94
2.11 DATA PROTECTION LEGAL FRAMEWORK AND THE GENERAL DATA PROTECTION REGULATION 95
3. CONCLUSION 97
IV. ACTUAL ACCESSIBILITY 99
1. INTRODUCTION 99
1.1 DIGITAL ECONOMY AND SOCIETY INDEX 100
1.2 DIGITAL DIVIDES 102

2. THE RESULTS OF THE EXPERT SURVEY 104

2.1 THE INDIVIDUAL 104

2.2 THE ECONOMY 104

2.3 DEMOCRACY 105

2.4 MEASURES 106

3. CONCLUSION 107

D. SUMMARY EVALUATION IN TEN THESES 108

PARTICIPATING EXPERTS 113

LITERATURE 115

LIST OF ABBREVIATIONS 123

APPENDIX: RECOMMENDATION CM/REC(2016)5 125

A. Introduction: Notion and Concept of Internet Freedom as per Recommendation CM/Rec(2016)5 and the Annex to this Report

The Internet is the virtual backbone of a digitally networked information society. The extent to which its state and benefits impact all areas of social coexistence and the realities of human life cannot be overestimated. This also affects the realisation of the values and goals of a liberal, democratic society, which is based on respect for fundamental freedoms and human rights. With these values in mind, the Committee of Ministers of the Council of Europe (CoE) have recommended to the member states that they perform regular evaluations on the basis of certain indicators, to determine to what extent the standards for human rights and fundamental freedoms are being respected and enforced with regard to the Internet. National reports should be prepared on this basis. These indicators are listed in the Appendix to Recommendation CM/Rec(2016)5. The involvement of all concerned parties from the economic, civil society and the academic and technological communities in their respective roles, should be ensured for this assessment and at the time of preparing the national reports. The Office of the Federal Chancellor (BKA), is arranging the preparation of such a national report on Internet freedom in Austria. The BKA has commissioned Prof. Walter Berka und Prof. Josef Trappel (both of the University of Salzburg) with the preparation of this report. The structure of this report is outlined in the following introduction; it proceeds from the notion and concept of Internet freedom.

The Committee of Ministers of the CoE define Internet freedom as 'the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the Convention'.[1] Consequently, the Recommendation is built upon a broad and integral concept that is based in the European catalogue of human rights; in this sense, Internet freedom is a freedom that should be realised through and on the Internet. The indicators devised in Recommendation CM/Rec(2016)5 also bear upon Internet freedom. They put into concrete terms the benchmarks that can be derived from the European Human Rights Convention and other standards of the Council of Europe. At the same time, the relationship established by the Committee of Ministers between the Internet and the human rights and fundamental freedoms of the Human Rights Convention, suggests that Internet freedom

[1] Recital 2 of Recommendation CM/Rec(2016)5 of the Committee of Ministers to the member states on Internet freedom

should be handled and evaluated primarily according to the aspects of the meaning that befit the Internet as a means of communication in the context of democratic societies, to which the Convention refers. This pertains to both individual communication options and media and mass-media communication using electronic communication networks. With this in mind, 'Internet freedom' should ensure advantageous general conditions for the exercise and enjoyment of fundamental freedoms and human rights in the online network of an information society.[2] This understanding also forms the basis of the following report.

The report comprises two parts. The first part addresses the general legal framework and standards in accordance with Austrian law with due consideration of the indicators listed in the Recommendation of the Committee of Ministers. The second part contains an empirical survey of the assessments and evaluations of the concerned parties from the economy, civil society and the academic and technological communities in accordance with Recommendation CM/Rec(2016)5 and ensures their involvement in the preparation of the national report. The conclusions evaluate the status of Internet freedom in Austria on the basis of the general legal framework and the compiled assessments by the concerned parties.[3]

Both authors are jointly responsible for the introduction and the conclusions of this report; the section on the general legal framework and standards was authored by Walter Berka and the empirical survey by Josef Trappel. References to the literature and the legal situation, respectively case law, are valid as of January 2018.

B. Internet Freedom in Austria: General Legal Framework and Standards

This treatment of the general legal framework for the realisation of Internet freedom in Austria focuses on the issues and indicators in Recommendation CM/Rec(2016)5. However, it deviates partially from the system of the recommendation to the extent that doing so seems reasonable for the purpose of better presentability. The respective

[2] Regarding the background, sense and purpose of Recommendation CM/Rec(2016)5, cf. the explanatory memorandum of the Steering Committee on Media and Information Society (CDMSI) dated 13/04/2016, CM(2016)26-addfinal. Regarding the significance of the Internet as 'one of the principal means by which individuals exercise their right to freedom of expression and information', cf. also the case law of the European Court of Human Rights (ECtHR), e.g. ECtHR 18/12/2012, No. 3111/10, Ahmet Yildirim, Sec. 54.

[3] A human-rights approach also underlies the 2013 collection of contributions in Landler, Parycek and Kettemann (ed.), *Netzpolitik in Österreich. Internet. Macht. Menschenrechte* (2013), which was published as a final report of a project implemented by Internet & Gesellschaft Co:llaboratory AT; http://publikationen.collaboratory.at/Co_Lab_MRI_NetzpolitikAT.pdf (accessed on 28/09/2017).

indicators to be taken into account are referenced in the form of marginalia. The cited legislation and abbreviations are itemised in the List of Abbreviations at the end of this report.

I. The constitutional and European-law framework

The following introductory section outlines the legal framework for the implementation of Internet freedom in Austria primarily by presenting the relevant guarantees under constitutional law (I.1.) and the general European legal framework (I.2.). Sections I.3. and I.4. outline the general regulatory framework for the Internet and the essential principles for enacting legislation and applicable policies with respect to the Internet.

1. Internet freedom and the human-rights guarantees of the ECHR

- The status of the European Human Rights Convention

Indicator 1.1.

The European Convention on Human Rights (ECHR) is assigned the rank of a federal constitutional law amongst Austrian legislation. It is thus a benchmark for the entire national body of laws below the constitutional level, and directly applicable rights that are guaranteed under constitutional law can be derived from it; these can be enforced by the Constitutional Court (VfGH) and the other supreme courts. Therefore, if the goal of Internet freedom is recourse to the human rights and fundamental freedoms guaranteed in the ECHR on the Internet, and the integral protection of these rights and freedoms in accordance with the Convention, then this is accounted for by the fact that the ECHR ranks at the constitutional level and by its direct applicability. Austrian law likewise thus accommodates the expectation expressed in the Recommendation of the Committee of Ministers that the fundamental freedoms and human rights guaranteed in the ECHR apply 'both offline and online'.[4] The guarantees of the Convention include the various aspects of Internet freedom, meaning, especially, the guarantee of free expression via the Internet, the protection of confidential communication on the Internet and the responsibility of the state to respect human rights in the context of communication transmitted via the Internet.

- Guaranteed fundamental rights of free speech and freedom of the media

[4] Recital 1 of Recommendation CM/Rec(2016)5 of the Committee of Ministers to the member states on Internet freedom; similar to Resolution 20/8 of the UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet', dated 16/07/2012; https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20 (accessed on 28/09/2017).

Indicator 1.2.

The protection of communication transmitted via the Internet is guaranteed primarily by the fundamental right to free speech as it is guaranteed in article 10 of the ECHR; this protection is supplemented by additional fundamental rights under national constitutional law (article 13 StGG, decision of the Provisorische Nationalversammlung [Provisional National Assembly]).[5]

Article 10 of the ECHR protects all forms of individual and mass communication, regardless of the technologies or communication channels used. This guarantee therefore applies to communication via the Internet.[6] This means that access to the Internet and communication via the Internet, including the free choice of communication content and the free receipt of content transmitted via the Internet, are protected by this fundamental right. Restrictions of this freedom to transmit and receive information using the Internet are permitted only under the conditions designated in article 10 paragraph 2 of the ECHR. This means that such limitations must be provided for by law, must protect a specific public interest or the rights of others, and they must be proportionate. This includes examining whether restrictions of free speech are appropriate, necessary and reasonable for achieving a legitimate goal; this must be assessed using the standards of a democratic society. In any case, censorship measures taken by the government are prohibited and unconstitutional; this absolute prohibition against pre-censorship, that is, preventative measures taken to control content, arises from a provision of national constitutional law. This prohibition of censorship is applicable to communication on the Internet.[7]

The following paragraphs will discuss the relevant provisions of basic statutory law and their relationship to the guarantees of the ECHR.[8]

- Guaranteed fundamental rights pertaining to the private sphere and data protection and the confidentiality of communication

[5] Regarding the legal bases and the guarantee of free speech in Austrian constitutional law, cf. Holoubek, *Kommunikationsfreiheit*, in Merten, Papier and Kucsko-Stadlmayer (ed.), *Handbuch der Grundrechte in Deutschland und Europa VII/1*[2] (2014), 591; Öhlinger and Eberhard, *Verfassungsrecht*[10] (2014), ref. no. 910 et seqq.; Berka, *Verfassungsrecht*[6] (2015), ref. no. 1452 et seqq.

[6] Cf. e.g. Berka, *Verfassungsrecht* (fn 5) ref. no. 1459; Holoubek (fn 5) 594.

[7] The prohibition of censorship arises from the decision of the 1918 Provisional National Assembly. It exceeds the requirements of article 10 of the ECHR because, according to the Convention, preventative measures are not absolutely ruled out; regarding the prohibition against censorship, cf. e.g. Holoubek (fn 5) 602; regarding the narrow limitations for preventative measures in light of art. 10 ECtHR, cf. e.g. ECHR 18/12/2012, No. 3111/10, Ahmet Yildirim, Sec. 47.

[8] Cf. section II.

The guarantees of the ECHR are also applicable to the protection of the confidentiality of individual communication transmitted via the Internet. Private and confidential Internet communication (e.g. emails, closed news groups, messenger services) is protected by the right to respect for one's private life and communication (art. 8 ECHR), and government encroachment on this communication is permitted only under the conditions stated in article 8 paragraph 2 of the ECHR. Such encroachment must therefore be provided for by law and required to achieve a legitimate goal. National fundamental rights supplement this protection, primarily through the fundamental rights of data protection (sec. 1 DSG) and the protection of telecommunications secrecy (art. 10a StGG), the latter predominantly due to the fact that judicial authorisation is required before official authorities can access the content of confidential electronic communication. However, as per prevailing practice and the case law of the Constitutional Court, telecommunications secrecy includes only the protection of content, whereas other information about an electronic communication (source, location and connection data) do not fall under the requirement for judicial authorisation.[9]

Indicator 1.2.

The following paragraphs will discuss the relevant provisions of basic statutory law and their relationship to the guarantees of the ECHR.[10]

- The protection of fundamental rights with regard to Internet communication

Indicator 1.2.

The state also bears a responsibility for respecting human rights in the context of Internet communication. In any case, such a responsibility is enshrined in constitutional law to the extent that positive duties to act can be derived from individual fundamental rights; for the state, this means that it must use the means available to it to ensure that fundamental freedoms and human rights are not violated via the Internet by non-governmental third parties. Such duties of protection are recognised as part of the right to respect of one's private life (art. 8 ECHR), above all with respect to protection against gross abuse or attacks on one's privacy. They can be derived from other guarantees of the ECHR, for example, from the protection against inhuman and

[9] Regarding art. 8 ECHR, cf. Wiederin, *Schutz der Privatsphäre*, in Merten, Papier and Kucsko-Stadlmayer (ed.), *Handbuch der Grundrechte in Deutschland und Europa VII/1*[2] (2014) 363; Berka, *Verfassungsrecht* (fn 5) ref. no. 1428 et seqq.

[10] Cf. section IV.

degrading treatment (art. 3 ECHR) or the imperative of respect for religious and ideological convictions of others as per article 9 of the ECHR.

Indicator 1.6.

A broad duty to penalise manifestations of cyber-crime cannot be taken from Austrian constitutional law. This is therefore part of the legal-policymaking responsibility of criminal-law legislators, which, however, is partially linked to European and international legal standards, for instance, with respect to combating hate propaganda or child pornography.

The following paragraphs will discuss the relevant provisions of basic statutory law and their relationship to the guarantees of the ECHR.[11]

- Regarding human rights protection in practice

The guarantees of the ECHR that are relevant to Internet freedom are observed and taken seriously in the practices of the Austrian courts. The case law of the European Court of Human Rights (ECtHR) is assigned a high degree of authority, and the Austrian courts follow it consistently. Contradictions between the requirements of the Convention and Austrian legal regulations are settled swiftly by the legislature as a rule.

The statement that Internet freedom is broadly protected and guaranteed by Austrian constitutional law is justified in this context. This does not rule out the possibility that there may be, in individual cases and certain contexts, discussions on whether the constitutional-law guarantees are effectively and properly enforced and sufficiently respected in practice. Such discussions are unavoidable and necessary in liberal societies and are a part of public social discourse regarding the realisation of human rights and fundamental freedoms. One example of such discourse, which can also include highly controversial positions, is the conflict between the effective preservation of freedoms on which a free society depends and protection from criminal and terrorist violence. This is also evident in the intense debates in Austria on the expansion of the surveillance powers granted to judicial and security agencies, which also inevitably impact the Internet.[12]

[11] Cf. section II.4.
[12] Cf. below, fn 97.

2. The European legal framework for Internet freedom

As Austria is a member state of the European Union (EU), EU law has primacy of application in Austria and is directly applicable, as appropriate. This also impacts the guarantee of Internet freedom.

Indicator 1.1.

Indicator 1.2.

- The Charter of Fundamental Rights of the European Union

Reference should be made chiefly to the guarantees of the Charter of Fundamental Rights of the European Union (CFR). The corresponding fundamental rights of the Charter – free speech and freedom of the media (art. 11 CFR), respect of one's private life and data protection (arts. 7, 8 CFR), and the freedoms of assembly and association (art. 12 CFR) – must be applicable domestically and with precedence for legislative acts that are enacted as part of the implementation of EU law (art. 51 para. 1 CFR). According to case law, the guarantees of the CFR may be asserted before the Austrian Constitutional Court (VfGH) as rights guaranteed under constitutional law; they form a standard of review in the general judicial review procedure, provided that their formulation and precision equate to those of rights guaranteed under the Austrian Federal Constitution.[13] This applies to all of the fundamental rights cited above, which on principal have the same meaning and scope as the corresponding rights of the ECHR.[14] As a result, the rights of the CFR are able to supplement and reinforce the guarantees of the ECHR, which apply domestically as constitutional law, and they also form a benchmark especially for the relevant law of the EU.

The nullification of the original European directive on data retention, which traced back to a request for an advance ruling of the Austrian Constitutional Court, represents an important example of the relevance of the Charter to the Internet.[15]

- Secondary legislation of the European Union

Apart from the Charter and other provisions of primary legislation, such as, particularly, the fundamental freedoms, there are numerous provisions of secondary legislation (directives and regulations) that significantly influence the legal position of the Internet. Because this legislation is also assigned precedence vis-à-vis Austrian national law, including constitutional law, these provisions are very relevant; they

[13] VfSlg 19.632/2012; regarding this verdict and its consequences, cf. Berka, *Verfassungsrecht* (fn 5) ref. no. 1198.

[14] Regarding the relevance of the CFR for the applicable fundamental and human rights in Austria, cf. Holoubek and Lienbacher (ed.), *Charta der Grundrechte der Europäischen Union. GRC-Kommentar* (2014).

[15] Cf. VfSlg 19.702/2012 and VfSlg 19.892/2014 in conjunction with ECJ 08/04/2014, C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, among others.

represent a binding legal framework for subordinate legislation (enforcement and application of EU law) and have a substantial impact on Internet freedom. Some important EU legal regulations that will be returned to in the further course of this report are referred to here only by way of an example:

- Regulation laying down measures concerning open Internet access – TSM Regulation (Regulation (EU) 2015/2120)
- Directive on audio-visual media services – AVMS Directive (Directive 2010/13/EU)[16]
- Directive on electronic commerce – Electronic Commerce Directive (Directive 2000/31/EC)
- General Data Protection Regulation – GDPR (Regulation (EU) 2016/679)[17]

3. General framework for the regulation of Internet communication

Indicator 1.5.

Austrian regulatory authorities, specifically the Telecom Control Commission and the Austrian Communications Authority (KommAustria), have been charged with the supervision and regulation of electronic communications services and certain online media. They are established as independent authorities (not bound by instructions);[18] their independence is based on a provision of constitutional law (art. 20 para. 2 B-VG). The independence of the ordinary courts (the criminal and civil courts), which are entrusted with matters pertaining to the Internet in various criminal- and civil-law contexts, is also guaranteed under constitutional law (art. 87 B-VG). These bodies are independent primarily vis-à-vis the national bodies, but other dependencies of an economic or political nature are also irreconcilable with their independence. Judicial legal protection is discussed in greater detail in section VI.

Insofar as the highest political administrative bodies (governments) and the authorities that are subordinate to them are entrusted with powers over the Internet, by their very nature they have no comparable independence. However, administrative acts of authorities can be challenged in the administrative courts, the independence of which is

[16] A new version of the Directive is in preparation; regarding the recommendation of the Commission, cf. COM(2016) 287 final; http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52016PC0287&from=EN (accessed on 28/09/2017), as well as the synopses of the recommendations of the Commission, Parliament and the Council of the Institute for European Media Law; https://www.emr-sb.de/gemischte-meldungen/items/emr-veroeffentlichtdeutschsprachige-synopse-zur-novelle-der-avmd-richtlinie-sowie-ersten-impuls-zum-anstehenden-trilogverfahre.html (accessed on 28/09/2017).

[17] Data Protection Directive 95/46/EC still applies until the GDPR comes into effect (25/05/2018).

[18] Sec. 116 TKG 2003; sec. 6 KommAustria-G; regarding the organisation of these institutions, cf. https://www.rtr.at/de/m/Institutionen and https://www.rtr.at/de/tk/Institutionen (accessed on 28/09/2017).

likewise guaranteed under constitutional law (art. 134 para. 7 B-VG) and which can also be invoked in the event of unlawful default by an authority.

4. Legislation with respect to Internet freedom

Legislative processes relating to the Internet are handled in legislative procedures that in general sufficiently take into account the imperatives of transparency and the involvement of concerned parties, primarily through corresponding evaluation procedures when laws are enacted.[19] Even if the involvement of community organisations in the law-making process is stipulated as mandatory only with respect to certain institutions (such as the chambers), on principle, it is at the discretion of each public political and civil society organisation to speak out in such procedures. Since the introduction of a new, expanded evaluation procedure in September 2017, authorities or persons who are not direct addressees of an invitation to the evaluation may also give opinions on laws proposed by ministries (ministerial draft bills). In addition, it is also possible to promote on Parliament's website opinions on a draft bill that have already been lodged. ***Indicator 1.4.***

In exceptional cases, an urgent political initiative may be lodged directly with Parliament using an initiative application, which can result in the omission of an expert evaluation; such a procedure is generally viewed critically by the political public and is therefore avoided whenever possible. Recently there was some criticism of this 'emergency procedure' during the passage of the Austrian law accompanying the GDPR.

Provisions and procedures of the regulatory authorities that impact the Internet are regularly discussed with the relevant stakeholders in transparent hearings.

The constitutionality of drafts, including their compliance with the ECHR, is reviewed regularly during legislative procedures, primarily by a special constitutional service established in the BKA. This ensures that legislation pertaining to the Internet is assessed during the draft phase with regard to the impact that its implementation may have on the exercise of human rights and fundamental freedoms. ***Indicator 1.3.***

[19] Regarding participation of concerned parties or other members of the public (advocates, NGOs) in the development of draft laws, this generally takes place once a first 'ministerial draft' prepared by the bureaucracy is sent for expert assessment, and also after the state or federal government takes a decision on a government bill. Regarding parliamentary handling of law initiatives, cf. the home page of the Austrian National Assembly, https://www.parlament.gv.at/ (accessed on 28/09/2017). Regarding the new, expanded evaluation procedure, cf. the relevant resolution of the National Assembly, 200/E, 25. GP; https://www.parlament.gv.at/PAKT/VHG/XXV/E/E_00200/fname_637132.pdf. (accessed on 28/09/2017).

II. Freedom of access to the Internet and the protection of free speech and freedom of the media on the Internet

Indicator 2.1

The issue of freedom of access to the Internet and the answer to the question of whether the Internet is available and accessible to and affordable for all segments of the population have legal and factual implications. Answers to legal questions associated with access to the Internet form the main topic of this part of this part of the study. (II.1). The section about regulation of online media under media law discusses the realisation of freedom of the media in the Internet (II.2.). The legal position of Internet platforms and so-called intermediaries has special characteristics (II.3.). Section II.4. discusses journalistic freedom in online media. The applicable restrictions on content that are most significant for Internet communication are presented following these sections and assessed in light of the fundamental freedoms and human rights (II.5.). Sections II.6. and II.7. discuss the principal of net neutrality and the problem of blocking in light of free speech and the right to receive and transmit information.

Information on the actual accessibility and availability of the Internet can be found in the part of this report that discusses communication studies.[20]

1. Freedom of access

- Legal framework

Indicator 2.1.1. Indicator 2.1.4.

Free access to the Internet is a fundamental condition of Internet freedom. With respect to the situation in Austria, it can be assumed that there are no legally significant barriers to access for private and commercial Internet users. They access the Internet within the framework of freedom of contract and private contractual relationships with Internet Service Providers (ISPs) that offer Internet connectivity using various technologies. The establishment of Internet access by an ISP itself represents the provision of a public communications service that requires only an announcement to the regulatory authorities but no official authorisation (sec. 15 TKG). The connection to the public communication network, including the transmission of data with data rates, that is sufficient for functional Internet access is a universal service that must be available at affordable prices (secs. 26 et seq. TKG).

ISPs are liable under contract vis-à-vis users, that is, they may not deny a contractual connection to a user without objective justification (sec. 69 TKG). General terms and

[20] Cf. section C.4. of this report.

conditions (GTCs) generally apply to the contractual relationship. They are subject to content control by the regulatory authorities and the courts. Within this legal framework, there are no limitations of Internet access. In the context of free access to the Internet, users may also make use of the services of the Internet without limitations, that is, they may create Internet content and make it available on the Internet themselves.

Indicator 2.1.8.

In the event of legal disputes between an ISP and users of Internet services, arbitration proceedings can be initiated with the regulatory authorities in which an attempt is made to reach an agreement between the user and the operator and to find a sustainable solution for conflicts (sec. 122 TKG). If the arbitration process concludes without a result, legal action must be taken in the competent court, which will conduct proceedings in compliance with article 6 of the ECHR.

Indicator 2.1.4.

If government authorities restrict Internet access for specific groups of persons or regions, corresponding restrictions will be taken as encroachments upon the freedom of information guaranteed in article 10 of the ECHR; they are lawful only if they are provided for under the law and serve an urgent social need. On principle, there are no restrictions of this kind under Austrian law.

Indicator 2.1.6.

Certain restrictions on Internet use may be imposed with respect to government institutions, such as in public schools or prisons. Within the penal system, the responsible institution head decides whether prisoners are permitted to use the Internet, to what extent this is permitted, and which controls are provided for from a security perspective. The law does not provide for any explicit legal right of access for prisoners; it must be decided on a case-by-case basis whether restrictions of Internet access are justifiable in general or in the case of specific services or websites. The decisions of the institution head are subject to scrutiny by the competent court, which, in the event of complaints, is guided by article 8 and article 10 of the ECHR and must reach a decision that takes into consideration the applicable case law of the ECtHR.[21]

The use of smartphones during instruction is often restricted or forbidden in schools. There is no explicit legal basis for this; pertinent orders from the administration may be

[21] Regarding the fundamental permissibility of the use of a computer, cf. the decision of the VwGH [Supreme Administrative Court] dated 08/05/2008, 2007/06/0231; it is clearly more restrictive in contrast with the so-called ‘computer decree’ of the Enforcement Administration of the Ministry of Justice dated 26/03/2014 (discussed in *Schöpfer*, *Entscheidungsanmerkung*, NLMR 2016, 60). Regarding the relevant case law of the ECtHR, cf. ECtHR 19/01/2016, No. 17.429/10, Kalda; ECtHR 17/01/2017, No. 21.575/08, Jankovskis.

based upon the school rules established by the school community bodies, upon the disciplinary powers granted to the bodies of the school or on the authority over the school granted under civil law.

2. The regulation of online media

Indicator 2.3

The fact that online media benefit from the fundamental protection of the freedom of the media ensured in article 10 of the ECHR, which ranks at the level of the constitution, has already been stressed in the preliminary treatment of this subject. Encroachments upon this freedom are therefore permitted only under the conditions stated in the guarantee of this fundamental right (art. 10 para. 2 ECHR).

Certain content distributed via the Internet is 'media' that is subject to specific legal regulation under the Media Act (MedienG) and the Audio-visual Media Services Act (AMD-G), as well as the law on public broadcasting (ORF-G). On the one hand, these laws contain certain regulatory actions, and on the other, they also contain regulations that bear on the content of online communications for the purpose of content regulation.

- The Media Act

'Periodic electronic media', which include, along with programs transmitted via broadcast, media that can be accessed using electronic means (websites),[22] recurring electronic media, or media that are distributed at least four times per year via electronic means, e.g. regularly distributed newsletters or YouTube channels, are subject to the MedienG.[23] Both cases assume the distribution of intellectual content to a larger group of people.[24]

Indicator 2.3.2.

The fact that the distribution of periodic electronic media does not require any official authorisation essentially applies to such media as a principle (freedom of distribution principle). The MedienG only stipulates compliance with specific regulatory actions: recurring electronic media must have a masthead, meaning that they must designate the name (company) and address of the media owner (sec. 24 para. 3 MedienG). Individual websites are not required to have a masthead, but, like the recurring electronic media, they must disclose their ownership structures and the basic orientation of the medium

[22] Sec. 1 para. 1 line 5a b) MedienG.
[23] Sec. 1 para. 1 line 5a c) MedienG.
[24] Regarding the relevant provisions of the MedienG, cf. e.g. Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar*[3] (2012).

(sec. 25 MedienG). Only limited disclosure is required for so-called 'private' or 'small' websites, that is, electronic media that do not purport to have influence on the shaping of public opinion (sec. 25 para. 5 MedienG). The collection by the Austrian National Library of periodic electronic media distributed via the Internet is also regulated by the MedienG, provided that these media are related to Austria; under certain conditions, the owners of such media themselves are obliged to submit them to the National Library (sec. 43b MedienG).

Along with these regulatory actions, the MedienG provides for certain special provisions for criminal proceedings in the event of media-content-related offences, meaning offences committed through the content of a medium (secs. 28 et seqq. MedienG). These provisions are also applicable to some extent to online media; they will be discussed in this study in the relevant contexts.[25] The regulations of the MedienG serve to protect personality rights via the right of reply, that is, the right of aggrieved parties to demand the rectification of false allegations (secs. 9 et seqq. MedienG). This claim is applicable to periodic electronic media with the exception of 'private' websites. Furthermore, the elements of compensation in the MedienG, which provide for civil liability of the media owner for certain encroachments upon the personality rights to respect of one's honour, privacy and presumed innocence, are significant (secs. 6 et seqq. MedienG). They also apply to publications on online media; these elements will be discussed further in the relevant factual context.[26]

However, liability is limited for postings from third persons that are uploaded to online discussion forums or rating platforms. On principle, the operators of such sites are liable only if they provoke unlawful postings through their own behaviour or do not delete these in a timely manner after becoming aware of them (sec. 16 ECG, sec. 6 para. 2 line 3a MedienG).[27]

- The law on audio-visual media services

Audio-visual media services are subject to separate media-law regulation through the Audio-visual Media Services Act (AMD-G). Along with traditional television (broadcasting), it concerns all audio-visual linear media services that are distributed via electronic communication networks (e.g. web TV, live streaming) and audio-visual on-

[25] Cf. section II.5.
[26] Cf. section II.5.
[27] Regarding the liability under media law of the operator of an online discussion forum on a website, cf. e.g. OGH 30/01/2017, 6 Ob 188/16i; OGH 21/12/2006, 6 Ob 178/04a.

demand services, such as video on demand.[28] In both cases, the law assumes that these media services come under the editorial responsibility of a media service provider. Therefore, according to the applicable legal situation, Internet platforms where the content is created by users (e.g. YouTube), do not fall under the AMD-G. However, the operator of a YouTube channel him-/herself can be considered a media service operator if the content that s/he distributes is comparable to that of a television programme.

Indicator 2.3.2.

The freedom of distribution principle applies to the audio-visual media services governed by the AMD-G within the context of a display system and in connection with certain regulatory actions. The content on offer by such a service must be shown to the regulation authority (KommAustria) and the intended service must be described. The exclusion of certain legal entities (legal persons under public law, political parties) from putting on television broadcasts and the restrictions for media associations that are provided for under the law (secs. 10, 11 AMD-G) do not apply to these services. Therefore, in comparison with the legal situation for traditional broadcasting, the freedom of distribution principle is accounted for to a far broader extent with respect to audio-visual media services.

Media service providers within the meaning of the AMD-G must observe certain regulatory actions; this includes, firstly, information about the name and address of the operator and designating contact options, as well as the duty to record the distributed content so that the regulatory authorities can inspect it (sec. 29 AMD-G).

Moreover, the law justifies certain limits on content for audio-visual media services through a content regulation; this includes the duty to respect human dignity and the rights of others, a prohibition against inciting hate (sec. 30 AMD-G), the duty to identify advertising in connection with certain advertising content prohibitions (secs. 31 et seqq. AMD-G) and restrictions on sponsoring and product placement. Special child-protection provisions apply to on-demand media services and linear media services, and television advertising is subject to further restrictions.

- Public service broadcasting

There are special legal regulations for the online activities of the Austrian Broadcasting Corporation (ORF), that is, for the public service broadcasting corporation that is

[28] Regarding the relevant provisions of the AMD-G, cf. Kogler, Traimer and Truppe, *Österreichische Rundfunkgesetze*[3] (2011) 399 et seqq.

charged with public service.[29] On principle, the ORF may also provide its television and radio programmes online, but the ability for users to save this content must be limited. Moreover, the ORF may also prepare an online offering of content, provided that this relates to the public service broadcasting programmes. However, the ORF-G (sec. 4f) makes a negative list of numerous online offerings that may not be offered by the ORF either under any circumstances whatsoever or within the context of its public-service task.

These regulations entail considerable restrictions for the ORF's Internet presence and on its social network pages. Whether these restrictions that were created in the interests of the market potential of private broadcasting corporations and the print media remain justified or whether they unreasonably hinder the presence and opportunities for development of public service broadcasting in a rapidly changing media world to the detriment of its task is the topic of an ongoing discussion and of relevant Supreme Court case law.[30]

3. Internet platforms and intermediary Internet services.

- Regarding the limited liability of the platform operator

There is presently no regulation under media law for networks and platforms with operators who do not discharge any editorial responsibility, that is, do not have any influence on the distributed content and the design of the overall offering apart from a selective ex-post control. This applies primarily to platforms for services that are generated by users, such as YouTube or Facebook. The Internet platform itself on which the distribution takes place can be based on the liability privileges of the Electronic Commerce Act (ECG).[31] First and foremost, the exclusion of liability of the hosting provider comes into play (sec. 16 ECG) so that the provider can only be held responsible once s/he does not delete or block access to unlawful information without delay after s/he is made aware of it. There is already comprehensive case law regarding

[29] Regarding this, cf. the relevant provisions of the ORF-G (secs. 3 para. 4a, 5 in conjunction with secs. 4e et seqq.); regarding these regulations. cf. Kogler, Traimer and Truppe (fn 28) 1 et seqq.

[30] Regarding this, cf. VfSlg case law 19.768/2013: repeal of the ORF-G regulation on the ban on links to and other cooperations with social networks (so-called 'Facebook ban') due to violation of the rights to free expression and free broadcasting; however, the ban on provision of a (separate) social network by the ORF is objectively justified with respect to the goal of protecting private competitors on the broadcasting market. Cf. further VfSlg 19.854/2014.

[31] Regarding the ECG, cf. Zankl, *ECG. E-Commerce-Gesetz*[2] (2016).

the scope and enforcement of this duty.[32] In the event of an evident 'hate post' on a Facebook page, for example, the courts have assumed that Facebook not deleting the post until one week after it was made aware of the post was too late and that the unlawfulness of the malicious comment was evident in any case.[33]

- Liability as a media owner

However, in many cases, the respective user who uploads content to platforms as a poster, blogger or video creator is considered a media owner within the meaning of the MedienG if s/he is responsible for the content's creation and performs the distribution or causes it to be performed him-/herself. The same applies to operators of moderated websites. Therefore, the profile owner of a Facebook profile is responsible for it under media law. These persons are thus liable as per the Media Act and carry the responsibility for compliance with other duties under media law. There also already exists extensive case law regarding this, primarily in connection with offensive attacks or invasions of privacy via publications on the Internet.[34] This liability of the media owner is limited if the content comes from third parties and has been provided on a website and the media owner of this website has not 'failed to take due care'.[35] This regulation primarily targets postings by third persons as they are made, for example, in the form of online readers' letters or entries on online discussion forums. From the perspective of the duties of care imposed by law on the media owner, there is no requirement to check user contributions in advance; rather, as a rule, there is also a requirement to delete the incriminated content without delay.

- Ongoing discussions

The significance of platform operators for community communication and communication culture has resulted in discussions on the expansion of the liability imposed on them, or expansion of the duty to delete unlawful or otherwise objectionable content. In this context, Austrian policy primarily anticipates a solution at the European level in which the European Commission primarily aims for a

[32] Cf. e.g. OGH 30/01/2017, 6 Ob 188/16i; OGH 21/12/2006, 6 Ob 178/04a, among others.
[33] OGH 22/12/2016, 6 Ob 244/16z.
[34] Cf. e.g. OGH 29/04/2015, 15 Os 14/15w; regarding liability for a Facebook account, OGH 25/05/2016, 15 NS 35/16i.
[35] Sec. 6 para. 2 line 3a, sec. 7 para. 2 line 5, sec. 7a para. 3 line 5, sec. 7b para. 2 line 4a MedienG; regarding this, cf. Berka, in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar*[3] (2012) sec. 6 ref. no. 40 et seqq.

corresponding voluntary commitment from platform operators, if necessary also in connection with procedures of the accompanying regulation.[36]

The expansion of the applicability of the European AVMS Directive to video platform services and the implementation of the modified Directive by Austrian law will mean that Internet services with operators who merely compile user-generated content without their own editorial responsibility will also be bound by this duty. According to the draft, video platform providers will be obliged to take suitable measures in their area of responsibility to protect minors from harmful content and to protect all citizens from incitements to violence or hate. This will result in co-regulation (regulated self-regulation).[37]

4. Journalistic freedom and independence in online media

- Independence vis-à-vis the state

Indicator 2.3.1.

The editorial independence vis-à-vis the state and policy of media that are active on the Internet is broad and securely guaranteed by the fundamental right to free speech and freedom of the media. This does not mean that government interventions in free and independent communication is completely ruled out, but such interventions regularly qualify as unlawful unless they have a constitutional, legal justification in each case.

Indicator 2.3.3.

Other forms of unfair exertion of influence by government institutions, in particular through threats, pressure or force, would likewise be unlawful. If such practices became known, significant public pressure and protest would also be expected, and this would likewise be the case for less obvious, subtler forms of attempted exertion of influence. More difficult to detect are attempts to influence media using economic power, including public funds, or through other informal means of government media relations or propaganda. Above all, the significant scale of advertising orders used by nearly all public institutions aroused a not-unjustified suspicion of massive influence of the media. The legislature reacted to this by obliging government authorities and other public institutions to report the sum of the funds used for advertising orders in the

[36] Cf. the communication of the Commission regarding online platforms on the domestic digital market - opportunities and challenges for Europe [*Online-Plattformen im digitalen Binnenmarkt - Chancen und Herausforderungen für Europa*], SWD(2016) 172 final; http://eur-lex.europa.eu/legalcontent/DE/TXT/PDF/?uri=CELEX:52016DC0288&from=EN (accessed on 28/09/2017).

[37] Regarding the draft of a modified AVMS Directive, cf. evidence above, fn 16.

media and the names of the media benefiting from this to the regulatory authorities each quarter, which would then publish these reports.[38] This duty also applies to all publications made on online media (audio-visual media services, periodic electronic media) in return for payment. This at least creates a certain amount of transparency regarding the public funds used for advertising orders. Along with this, there are also certain restrictions on content for paid advertising orders made by public institutions, which essentially may have factual information as their object only to satisfy a specific need of citizens for information on the subject.

- Freedom of occupation for journalists

Indicator 2.3.1.

The independence of the media must be protected not only vis-à-vis the state and government authorities, but also vis-à-vis pressure and impermissible exertion of influence from other interest groups so as to fulfil the expectation of the public that the shaping of opinion be diverse and that reporting be objective. Traditional media law has assured the right to a certain journalistic freedom to media personnel who are active in print media and broadcasting in order to enable them to discharge their journalistic duties professionally and responsibly. This ensures that journalists have a sphere of freedom within the media companies for which they work.

Discussions in these contexts often focus on freedom of occupation for journalists in the sense of an 'inner freedom of the media'.[39] These rights were and are designed to be professional rights, that is, they presume regular professional activity in a journalistic field.[40] Within this scope, they can also benefit professional creators of online media.

Media personnel in online media that are subject to the MedienG and who thus participate professionally in the creation of content for websites or periodic on-demand services[41] can invoke the protection of the right to one's convictions as per secs. 2 et seqq. of the MedienG. They therefore have the right to refuse to collaborate on the content creation of postings or presentations that contradict their beliefs in fundamental issues or the principles of the profession of journalism; they may not suffer any detriment resulting from such refusal. If a posting that is created by such media

[38] Media Cooperation and Funding Transparency Act, BGBl I 2011/125, as amended, BGBl I 2015/6.
[39] Cf. Holoubek, *Innere Rundfunkfreiheit*, in: Berka, Grabenwarter and Holoubek (ed.), *Unabhängigkeit der Medien* (2011) 133.
[40] Regarding this, cf. the definition of 'media personnel', sec. 1 para. 1 line 11 MedienG.
[41] Regarding this, cf. the definition of 'media personnel', sec. 1 para. 1 line 11 Media Act.

personnel is subsequently modified in a way that pertains to its meaning, then it may be published under the creator's name only with that person's permission.[42] Additional rights of journalistic freedom in the sense of an 'inner freedom of the media' can be agreed in the editorial regulations (sec. 5 MedienG) that exist in individual Austrian media companies. Media personnel in audio-visual media services as per the AMD-G also have a right to the protection of their beliefs under the MedienG if the service is either a website or a recurring electronic medium within the meaning of this law.

Special rights of journalistic freedom apply to employees of television programmes and shows that are broadcast online and employees of the ORF who participate in the creation of online offerings at the public service broadcasting corporation in a programme-designing or journalistic capacity. Companies must respect their independence and self-reliance; journalistic personnel must not be made to write or take responsibility for anything that contradicts their freedom to practice their profession. The particulars of these guarantees and additional participation rights are governed by editorial bylaws; they must be bindingly negotiated between the company and the representatives of the journalistic employees (sec. 49 AMD-G, secs. 32 et seq. ORF-G).[43] Of course, the freedom to practice the profession of journalism is not without its limits; rather, it can be restricted within media companies through the administrative powers of the company management or editorial supervisors, primarily when the restriction concerns the journalistic profile and task of the media company. A right of the employee to transmit or distribute a specific posting cannot be derived from this freedom.[44]

- Protection of journalistic sources and editorial confidentiality

The editorial confidentiality governed by the MedienG is also conceived as a professional right for journalists that is assigned (only) to media owners, media personnel and employees of media companies (sec. 31 MedienG).[45] These persons are granted a right to refuse to give evidence, that is, as witnesses in court cases they may withhold the names of their sources and the information given to them. This right serves the protection of journalistic sources, that is, it protects the confidentiality of the

[42] On these rights and their limitations, cf. Noll, in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar* (2012) sec. 2 and sec. 3.
[43] Regarding this, cf. Kogler, Traimer and Truppe (fn 28) 311 et seqq., 541 et seqq.
[44] Regarding the journalistic freedom of ORF employees for this purpose cf. VfSlg 19.742/2013.
[45] Regarding editorial secrecy, cf. Heindl, in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar* (2012) sec. 31.

relationships between journalists and their informants, which is seen as a condition that is required to allow the media to perform their task of 'public watchdog'.[46] It is for this reason that the operator of an online daily newspaper, as a media owner, may refuse to disclose the data of a user who has posted confidential information on the daily newspaper's Internet forum.[47]

Apart from media owners, the employees of online media can also invoke editorial secrecy and protect their sources. Indeed, media personnel are the only ones who practise a journalistic profession (not necessarily full-time) in the context of a media company; anyone who is not active in a media company as media personnel or another type of employee does not have the right to refuse to speak out. This means that someone who publishes on the Internet as, for example, a blogger or a poster but who does not do so in his/her capacity as an employee of a media company may not invoke editorial secrecy. Of course, users who create the content of an online medium and distribute it themselves may be considered to be media owners, for example in the context of operating a Facebook account or as the moderator of a discussion forum. In this capacity, they have the right to editorial secrecy.

It seems doubtful whether the privileging of professional journalism remains justified in view of the changed circumstances and the significance of 'citizen journalism'.

The general surveillance of the Internet activity of citizens by police and judicial authorities may result in restrictions to the protection of journalistic sources.[48]

- The protection of journalists and other stakeholders on the Internet

Indicator 2.3.6.

Aside from the professional journalistic rights presented above, journalists and other persons who actively publish on the Internet are entitled to the full and unrestricted protection of the legal system in general. There are no known incidents in which a concerned party was denied this protection or in which an investigation was not launched immediately and, if necessary, criminal proceedings were not initiated in response to an encroachment. This does not rule out the possibility of public discussions on the achievements and mistakes of media or media personnel, especially

[46] Regarding the current significance and scope of the protection of journalistic sources, cf. OGH 16/12/2010, 13 Os 130/10g.

[47] OLG Vienna 26/02/2013, 19 Bs 504/12z, MR 2013, 61. Otherwise, a civil judgment that denies the protection of editorial secrecy for posts that were published without the activity, scrutiny or notice of a member of media personnel and on the user's own impulse; OGH 21/01/2014, 6 Ob 133/13x.

[48] Regarding this, cf. below, section V.2.

in relation to their activities on the Internet. In general, the reaction of the Austrian public when attempts by politicians or other pressure groups to exert influence over journalists have come to light has been thoroughly sensitive and critical, especially in matters concerning the independence of journalists employed in public service broadcasting.

Indicator 2.3.5.

There is no specific protection for online media from cyber-attacks or other disruptions to their ability to function. The media and other communications services certainly also benefit from the intensified efforts of Austrian authorities and companies to counter these threats in the most general sense. There are no documented cases of attacks of this kind aimed at online media or specific websites.

5. Content restrictions in Internet communication and online media

Communication transmitted by means of the Internet in general and the content of online media in particular are subject to legal restraints that are enacted by the competent legislature for the purpose of 'content regulation' in the public interest or to protect the rights of others. This is often expressed to the effect that what is prohibited offline is also prohibited online. It is not possible to go into the various restrictions in detail as part of this study. What is primarily of interest here is the assessment of these restrictions in light of the fundamental freedoms and human rights, for which reason current individual contexts will be discussed using examples.

- Content regulation and article 10 of the ECHR

Indicator

The starting point must be the observation that each instance of exertion of influence by the government on the content of Internet communication amounts to a restriction of free speech and the freedom of the media guaranteed in article 10 of the ECHR, and this regardless of whether the government prohibits certain content or stipulates specific communication content for the users of the Internet. To this extent, these fundamental rights guarantee the autonomy of communication made by means of the Internet. Government encroachments upon this autonomy are therefore permitted only under the conditions stated in article 10 paragraph 2 of the ECHR. This applies both to criminal prohibitions and to civil restrictions. On the other hand, the government may also have duties of protection in the interest of the rights of others, for the protection of which the legislature must prohibit or regulate certain content and

forms of communication if such content or forms of communication violate fundamental freedoms and human rights.

These connections between the regulation of the content of Internet communication and the fundamental rights are given due consideration throughout Austrian legal practice. The question of whether article 10 of the ECHR is taken into account when legal restrictions are enacted is already regularly considered during the legislative process; the Constitutional Court examines the constitutionality of laws that restrict fundamental rights as part of the powers granted to it, and it repeals legal provisions if these curtail free speech and freedom of the media in a way that contradicts the constitution. The application of laws is also subject to scrutiny by the courts, not just with respect to the legitimacy of enforcement but also in light of free speech and freedom of the media.

- Limitations under criminal law in the public interest

This applies to criminal-law limitations of communication made by means of the Internet, which are only constitutional if the penalisation of certain utterances or representations is absolutely necessary to protect overriding community interests. Some examples of this are prohibiting 'hard' pornography and any form of child pornography,[49] making incitement to or endorsement of terrorist acts punishable,[50] ensuring religious peace as part of the definition of the criminal offence of disrupting the practice of religion[51] or prohibiting the denial, downplay or justification of Nazi crimes against humanity ('Holocaust denial').[52] Freedom of speech must also be taken into account on a case-by-case basis when these offences are enforced. For example, it is recognised that the range of free choice guaranteed by free speech (or artistic freedom), which also guarantees freedom of harsh satire or polemic criticism, must be carefully taken into account when caricatures or satirical statements that criticise or mock religious content are assessed under criminal law.[53]

[49] Cf. the offences defined in the Bundesgesetz über die Bekämpfung unzüchtiger Veröffentlichungen und den Schutz der Jugend [Federal Act on Combating Indecent Publications and the Protection of Youth against Moral Hazards], BGBl 1950/97, as amended, and secs. 207a et seqq. StGB.

[50] Cf. sec. 282a Criminal Code.

[51] Cf. sec. 188 Criminal Code.

[52] Cf. secs. 3g, 3h of the Prohibition Act of 1947, which ranks at the constitutional level, Criminal Code 1945/13, as amended.

[53] Cf. e.g. OGH 11/12/2013, 15 Os 52/12d regarding a judgment of interference with religion (vilification of the prophet Mohammed) in light of free speech (with extensive reference to the case law of the ECtHR).

- Personality protection

The focus on the fundamental freedoms and human rights plays a significant role in the making and application of laws where the protection of human personality rights is concerned. The two dimensions of the fundamental rights also come to bear here; on the one hand, regulations to protect honour and privacy or guarantee presumed innocence limit free expression via the Internet, and on the other hand, it is recognised that these personality rights could face an entirely new kind of threat due to the omnipresence, boundlessness and uncontainable options for information storage of that same Internet, which obliges the legislature to ensure appropriate protection.[54]

There are corresponding regulations in the protection against abuse (defamation, verbal abuse, slander) contained in criminal law, the civil charges to protect honour and privacy (libel, damage of credit, right to one's own image) and, above all, in the civil elements of compensation contained in the MedienG, which form the basis for liability of the media owner for encroachments on honour, privacy or the presumption of innocence.[55] If there are still loopholes in the area of personality protection, these can be closed with section 16 of the ABGB, which guarantees general protection of the 'inborn rights', that is, the personality rights; the elements of this offence are also applicable in light of the fundamental freedoms and human rights. So, for example, in a recent decision the Austrian Supreme Court of Justice was able to infer from this provision a legal right of the individual not to be photographed in a way that violates his/her rights; the court supplemented its support of this claim based on article 8 of the ECHR and referred to the risks inherent in the distribution and manipulation possibilities of modern digital technology, among others, to justify it.[56]

The addressed offence definition for the protection of personality rights also applies to the various manifestations of Internet communication, either in general (such as the general offence definitions under criminal and civil law) or (as with claims for compensation under media law) in the case of online media that are subject to the MedienG.[57] In practice, the Austrian courts are assigning an ever greater importance to

[54] Regarding the government duty of protection, cf. VfSlg 14.260/1995.

[55] As an overview of the various defined offences against personality protection, with additional references to criminal and civil literature and case law, cf. Berka in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar*[3] (2012) *Vorbemerkungen* secs. 6-8a.

[56] OGH 27/02/2013, 6 Ob 256/12h.

[57] Regarding this, cf. above, fn 22 et seqq.

proceedings connected with publication via online media or other forms of communication via the Internet (blogs, postings, etc.).

Indicator 2.4.2.

In all of these contexts, it is ongoing case law that must interpret and apply the relevant elements of offences in light of the fundamental freedoms and human rights, which generally (primarily in the case of personality protection under civil law) results in a weighing of interests between free speech and opposing rights, such as the right to respect of one's privacy; this weighing of interests focusses on the affected fundamental rights. This focus on fundamental rights and on the associated relevant case law of the ECtHR manifests itself in various established standards and precepts of interpretation, which are referred to only by way of an example here: the imperative of a strict distinction between allegations of abuse, for which there is a liability if the facts claimed by the accused are false, and value judgments, which it must be possible to make without punishment on principle. The status of an attacked person must be taken into account because protection from abusive attacks on private persons is stronger than that for 'public figures'. When instances of exposure of one's private life or other cases of exposure of a person are evaluated, it must be examined whether or not such exposures have contributed to a matter of public interest or public significance.[58]

In this way, it is guaranteed, on principle in any case, that the strict focus on the fundamental freedoms and human rights assures the range of free choice that is due to communication by means of the Internet based on the ECHR, and likewise that the rights of people who have been victims of attacks via the Internet that violate their human dignity and fundamental rights to freedom are guaranteed. At the same time, the scrutiny of government authority and criticism of government bodies is assured the corresponding freedom. The focus on article 10 of the ECHR and the relevant case law of the ECtHR guarantees that no excessive penalties or compensation obligations are imposed during the application of laws against abuse and other defined offences against personality rights on the Internet. However, legal regulations such as the limitation of the amounts of compensation that can be imposed in the event of attacks on personality rights as per the provisions of the MedienG also contribute to this.

[58] Regarding these and other established standards, cf. e.g. Berka, *Persönlichkeitsschutz und Massenmedien im Lichte der Grundfreiheiten und Menschenrechte*, in Koziol and Warzilek (eds.), *Persönlichkeitsschutz gegenüber Massenmedien. The Protection of Personality Rights against Invasions by Mass Media* (2005) 493; regarding the adoption in Austrian practice of the applicable assessment criteria developed by the ECtHR, see Berka, *Ein „bewegliches System" des Persönlichkeitsschutzes: zur jüngeren Judikatur des EGMR zu Art 10 EMRK*, Journal of Information Law 2013, 154.

The enforcement of personality rights protections in the event of malicious attacks on the Internet poses problems and leaves open questions. This discussion will return to that topic.[59]

- Cyber-stalking and cyber-bullying

The Austrian legislature has reacted to new forms of persistent harassment of and compromising injury to persons that are at least facilitated and benefited by the Internet by legislating its own criminal offences. The common denominator between these is that they are attacks that can result in the violation of human dignity. 'Stalking', that is, persistently pursuing a person in such a way as to have an unreasonable negative impact on the victim's lifestyle, has already long been punishable; this also includes when contact is made with the victim using Internet services (sec. 107a StGB). 'Cyber-bullying' has been punishable since 2016; the description of this offence is paraphrased as 'continuous harassment using telecommunications or a computer system'. This offence is committed by anyone who injures the honour of a person on the Internet in a way that is perceptible to a large number of people, or makes highly personal facts or images available to a large number of people; in both cases, it is expected that these events occur over a long period of time and that they can have an unreasonable negative impact on a person's lifestyle (sec. 107c StGB).

- 'Hate speech' and 'fake news'

Malicious attacks on minors and other vulnerable social groups or on outsiders to the community can also violate human dignity and result in discrimination against vulnerable groups of persons. The Internet has provided a space for aggressive, misanthropic 'hate speech' that is difficult to control, which is cause for concern. This applies comparably to the distribution of false rumours, false reports and computer-generated bots, which multiply on the Internet with furious rapidity. They can poison public discussions on important societal issues, endanger the accuracy of democratic elections and manipulate people. Such phenomena show the 'dark' side of the Internet, through which human rights can be violated and democratic discourse can be corrupted more or less without restraint. From this perspective, the legislature has a human-rights-based responsibility to oppose such aberrations, which are a threat to human dignity and freedoms.

Indicator 2.4.3.

[59] Cf. section VI.

Certain manifestations of 'hate speech' violate applicable Austrian law. Distributing false, abusive allegations, attacking people with abusive criticism and mocking them violate personality rights that are protected under criminal and civil law. These have already been discussed above. The protection of the right not to be abused also benefits groups comprising a closed, manageable circle of persons.[60]

Moreover, certain severe forms of incitement are punishable under criminal law as per section 283 of the Criminal Code; the elements of this offence are expanded by the Criminal Code Amendment Act of 2015 and have been adjusted to fit the requirements of the corresponding European framework decision.[61] According to this, anyone may be punished who does the following, publicly and before many people:

- Calls for violence or incites hate against specific designated institutions (churches or religious communities) or groups of persons who are identified by certain social characteristics[62] or members of such a group;[63]
- Berates a protected group with the intention of violating human dignity, if this makes the group contemptible or degrades them in public opinion;
- Condones, denies, grossly makes light of or justifies certain crimes (genocide, crimes against humanity, war crimes, aggression), provided that this behaviour is directed at one of the protected groups or a member of such a group and is likely to incite violence or hate against them;
- Moreover, distributing written material with ideas or theories that endorse, promote or incite hate or violence against one of the protected groups is also punishable.

When the elements of these offences are applied, the fundamental rights of free speech and freedom of the media must also be respected, meaning that neither polemic nor satirical discussion may be punished, and critical or even provocative discussion of historical events must not be prevented. It is therefore crucial that the ramifications and consequences of punishable incitement as per the offence definition in section 283 of the Criminal Code – primarily when the offence is a call for violence, incitement of hate or the violation of human dignity – be carefully reviewed in order to avoid the criminalisation of free expression while, at the same time, vigorously opposing attacks

[60] Regarding disparagement of concentration camp victims, cf. most recently OGH 29/11/2016, 6 Ob 219/16y.

[61] Framework decision 2008/931/JI on combating certain forms and expressions of racism and xenophobia under criminal law, OJ L 328, 55. Regarding the revised version of sec. 283, cf. e.g. Lendl, *Von Weblogs, Userforen und sonstigen Kommentaren im Web – Strafrechtliche Grenzen und Haftung nach dem MedienG*, in Berka, Holoubek and Leitl-Staudinger (ed.), *BürgerInnen im Netz* (2016) 47 (48 et seq.).

[62] According to sec. 283, protected groups are defined by the following characteristics: race, skin colour, language, religion or ideology, citizenship, ancestry or national or ethnic origin, gender, physical or intellectual disability, age, sexual orientation.

[63] Regarding anti-Semitic harassment on Facebook, cf. e.g. OGH 22/07/2015, 15 Os 75/15s.

on human dignity. It must be acknowledged that drawing such boundaries in light of the vague offence definition in section 283 of the Criminal Code is not always easy.

Considering the verifiable increase in brutality of communication on the Internet, the question of whether further legal measures need be taken beyond the existing defined offences against personality rights and incitement in order to be able to take legal action against hate speech and advocating violence on the Internet, remains open.[64]

This also applies to the problem of so-called 'fake news'. The distribution of false rumours and manipulated news on the Internet violates existing legislation only in exceptional cases, such as when false news is distributed during an election period or referendum (sec. 264 StGB). Another pertinent offence definition that penalised the distribution of false, unsettling rumours with the prerequisite that this would perturb a large group of persons and disrupt public order was repealed in 2015. It is also the subject of an ongoing discussion of whether there should be energetic intervention against the manipulation of opinion formation in the interest of securing the foundation of a democratic decision-making process. Certainly, much depends on whether the services of professional journalism and the traditional media are still able to provide objective reporting and a pluralistic diversity of opinions to a sufficient extent even under the current altered conditions. It must be clear that it is all too easy for government or judicial control of the 'truth' or 'objectivity' of societal communication to cross the line into dangerous interference with free speech and freedom of the media.

6. Implementation of the net neutrality principle

Indicator 2.2.3.

Ensuring unhindered and discrimination-free access to the Internet forms the basis of the principle of net neutrality. In Austria, this principle is ensured by the validity and direct applicability of the EU Regulation laying down measures concerning open Internet access (TSM Regulation (Regulation (EU) 2015/2120)) and as part of the conditions and restrictions governed by this Regulation. The central provision is the obligation to treat all data traffic equally when Internet access services are provided. This obligation corresponds to a parallel claim of end users. They have the right to

[64] In this context, cf. the recommendation for a new criminal offence definition that, supplementary to sec. 283 of the Criminal Code and in enforcement of the supplementary protocol to the Convention on Computer Criminality, is also meant to impose administrative criminal sanctions on the distribution of racist and/or xenophobic discrimination propaganda; regarding this, see initiative proposal 2242/A, 25. GP.

access and distribute information and content and to use and provide applications and services via their Internet access services without discrimination.

The principle of treating data traffic without discrimination can be breached according to the Regulation as part of specific traffic-management measures and for the benefit of special services, the conditions and limits of which are defined in the Regulation (art. 3 TSM Regulation). On principal, the measures of appropriate traffic management provided for must be transparent, non-discriminatory and proportionate, and they must not be based upon commercial considerations, but rather only upon objectively varying technical requirements of the service quality of specific data-traffic categories. The specific content of data traffic may not be monitored with these measures, and they must not be in place any longer than is necessary. Further measures are permitted in exceptional cases, such as for blocking illegal content, if this is provided for under Austrian or EU law. However, since these measures interfere with the fundamental rights and freedoms that are enshrined in the ECHR and the CFR, such restrictions may be imposed only when they are appropriate, proportionate and necessary within a democratic society and their application is subject to appropriate procedural safeguards, including the right to effective legal protection and a fair trial.[65]

In their (first) net-neutrality report in 2017, the Austrian national regulation authorities refer to some problems that have been resolved or are still being resolved with the realisation of the net neutrality principle (e.g. zero rating, qualification of video on demand as a special service), but it assesses the initial experiences with the legal situation created by the Regulation as positive overall.[66]

A current draft bill that empowers the ISPs to take traffic security measures in accordance with article 3 of the TSM Regulation in order to prevent, very generally stated, ‘criminally relevant activities’ has provoked justified concern. This authorisation is extremely vague because the illegal content that would be under consideration is described only vaguely and by way of an example; the question also remains open of whether effective legal protection that takes into account freedom of

[65] Cf. recital 13.
[66] https://www.rtr.at/de/inf/NNBericht2017/Netzneutralitaetsbericht_2017_RTR.pdf (accessed on 28/09/2017).

information for the affected users is guaranteed when content is blocked based on this authorisation.[67]

7. Blocking Internet access and deleting content from the Internet

- Blocking

Indicator 2.2.1.
Indicator 2.2.4.

Blocking or otherwise restricting access to Internet platforms (social media, blogs, websites) or to information and communication technology tools such as instant messaging constitutes a grave encroachment on the free speech and freedom of the media. This applies with respect to both aspects of these fundamental rights, that is, both in view of active freedom of expression and in view of the freedom of users to receive information.

There is no general authorisation under Austrian law for government institutions to block access to the Internet or Internet services, and the introduction of such measures is not up for discussion.

The problem of blocking was thus ignited by the blocking of websites by ISPs for the purpose of preventing violations of copyright law on the Internet. The starting point for this is the regulation of section 81 paragraph 1a of the Copyright Act (UrhG), which gives the rights-holder a claim to injunctive relief that can also be enforced against the intermediary, whereby both the access provider and the hosting provider are considered intermediaries within the meaning of this provision pursuant to the case law of the ECJ.[68] It is therefore permissible on principle to prohibit ISPs from allowing customers to access specific websites (e.g. kino.to) with a court order in order to protect rights-holders. According to case law, users do indeed have a right not to be prevented from accessing lawfully available information in spite of the blocking, which they can assert in court with an appeal to their freedom of information – as stipulated by the ECJ.

On the basis of this case law, human rights requirements can be taken into account on principle as part of a necessary weighing up between the interests of creators and other rights-holders, which are protected under basic law, and the rights of content providers and access providers, and this primarily in view of the impaired freedom of information

[67] Cf. sec. 17 para. 1a Telecommunications Act according to draft 326/ME 25. GP.

[68] Cf. OGH 24/06/2014, 4 Ob71/14s in conjunction with ECJ 27/03/2014, C-314/12, UPC Telekabel Vienna GmbH; cf. further OGH 21/10/2014, 4 Ob 140/14p; OGH 19/05/2015, 4 Ob 22/15m; ECJ 14/06/2017, C-610/15, Stichting Brein/Ziggo BV, XS4ALL Internet BV.

of the users affected by the blocking.[69] The imperative of judicial scrutiny is likewise complied with on principle. Specific uncertainties of the legal situation and difficulties presented by legal enforcement must be established, and they burden primarily the ISPs with certain risks. The judicial legal protection that is granted to Internet users on principle can also be confronted with practical problems and not insignificant costs for implementation. When the assessment is made, the broad leeway that is afforded the Austrian legislature in this conflict area under legal policy according to the applicable case law of the ECtHR must indeed be taken into account.[70]

Indicator 2.2.5.

The government has not provided any information about blocked websites or other official restrictions of Internet access. Of course, this must be viewed in a context where there is no systematic blocking, banning or filtering of Internet content or Internet services by authorities in Austria in any case.

- Deletion of Internet content

Indicator 2.2.2. Indicator 2.2.4.

Punishable content on the Internet can be deleted by order of the competent media court if the deletion of the location of a website that forms the basis of the punishable action is recognised in a punitive sentence for a media-content offence. Such deletion can also be decreed in so-called independent proceedings if the objective elements of the offence constitute a punishable act and it is not possible to track a specific person (sec. 33 MedienG).[71] The deletion should prevent the continued influence and further distribution of punishable content. Online media includes only websites and not mass emails or newsletters because these are not distributed on an ongoing basis in the same way as websites. A weighing of interests is not provided for, which means that, when there is deletion, it must be ascertained if there is a conviction due to a media-content offence and that the prosecutor requests it.[72]

Deletion can also be decreed as a preventative measure if it can be assumed that a conviction will occur (sec. 36 MedienG). The court may order deletion merely as a preventative measure only if the negative consequences of the deletion are not disproportionately severe in comparison with the interest of legal protection that the

[69] However, regarding the current draft with a farther-reaching and not unproblematic authorisation for blocking, cf. the evidence above in fn 67.

[70] Cf. e.g. ECtHR 19/02/2013, No. 40.397/12, Fredrik Neij and Peter Sunde Kolmisoppi.

[71] Regarding the deletion and independent procedure under the media law and regarding temporary deletion, cf. Heindl in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar*[3] (2012) sec. 33 and sec. 36.

[72] As its only restriction, section 33 paragraph 2a of the MedienG states that deletion is not permitted if the utterance of a third party is reproduced on a website and there is a public interest in this reproduction.

deletion is meant to serve. If the legal protection interest can also be met by the suggestion of initiation of criminal proceedings, then the preventative deletion is not permitted.

The deletion of Internet content according to these provisions is ordered by the court (media court) and can be contested by a superior court; if there is a claim of violation of fundamental freedoms and human rights, it can also be contested through a petition to the OGH (sec. 363a para. 1 StPO). The possibility of verifying the lawfulness and proportionality of these measures is ensured in this way.

III. The freedoms of association and assembly and the Internet

1. The protection of the freedoms of association and assembly with regard to the Internet

Indicator 3.1.

Indicator 3.2.

Indicator 3.3.

The freedoms to assemble and to create associations are constitutionally guaranteed in Austria by article 11 of the ECHR and article 12 of the CFR, which rank at the constitutional level, and by the corresponding fundamental rights of the national fundamental rights catalogue.[73] The formation of associations, including unions, and the implementation of assemblies are permitted without official approval and require only a relevant announcement to the competent authorities. These freedoms also protect activities on the Internet.

This means that the affiliation of people for the purposes of an association in order to operate Internet platforms is as much the object of protected freedom of association as is the use of Internet services by associations, be it to exercise their right to free expression, to organise the activities of an association or to advertise such activities. This also applies to the use of Internet platforms or other Internet services to organise or advertise for assemblies for any desired purpose. As is shown by the option to create citizen's initiatives and petitions that can be lodged and supported at the federal level and, in some countries, even online, citizens are in fact making use of a form of democratic 'e-activism'.[74] Austria occupies a leading position with respect to electronic government strategies and practices, respectively electronic participation.[75]

---

[73] Regarding an overview of the freedoms of association and assembly, cf. Berka, *Verfassungsrecht* (fn 5) ref. no. 1497 et seqq.

[74] Although citizen's initiatives and petitions must be submitted in writing to the National Assembly of Austria, citizens can approve these electronically, thus supporting them; cf. https://www.parlament.gv.at/HILF/EZUSTIM/ (accessed on 28/09/2017); regarding the legal situation in the state of Vienna, where petitions can be lodged

2. Restrictions of the freedoms of association and assembly

Indicator 3.4.
Indicator 3.5.

Encroachments on the freedoms of association and assembly by government authorities are permitted only if they are provided for under the law and remain proportionate. On principle, the applicable laws provide for only certain regulatory actions. Prohibiting or dissolving assemblies or government dissolution of associations is permitted only in specific, legally stipulated cases and as a last resort.[76] Official encroachments are subject to judicial scrutiny by the administrative courts and the Constitutional Court. In accordance with the ongoing case law of the Constitutional Court, the authorities must observe the conditions for an encroachment stated in article 11 paragraph 2 of the ECHR – there must be a legitimate goal, an encroachment must be necessary and proportionate – for all of their decisions.[77] According to this case law, the authorities are moreover obliged to use appropriate means to prevent third parties from disrupting lawful assemblies.[78]

As a result, it is primarily this case law that ensures that use can be made of the fundamental rights of freedom of association and freedom of assembly in a broad manner and in conformity with fundamental freedoms and human rights. This also applies to all cases in which these freedoms are used in connection with Internet activities. There are no reports on government measures that would result in restrictions to Internet use in connection with the right to associate or assemble freely and peacefully with others.

A 2017 amendment strengthened the regulatory actions of the Public Meetings Act. However, this amendment, which extended the time periods to be observed when reporting assemblies, for example, has no impact on the freedom of the Internet.[79]

---

electronically, cf. https://www.wien.gv.at/amtshelfer/dokumente/verwaltung/wahl/petition/einbringen.html (accessed on 28/09/2017).

[75] Cf. Ringler, among others (ed.), *Internet und Demokratie in Österreich* (2013) 12 et seqq.; available at http://archiv.bundeskanzleramt.at/DocView.axd?CobId=53351 (accessed on 28/09/2017).

[76] Regarding banning and dissolving assemblies, see secs. 6, 13 of the Public Meetings Act (VersG); regarding banning and dissolving clubs, see secs. 12, 29 of the Associations Act (VerG).

[77] Cf. e.g. VfSlg 19.852/2014 regarding freedom of assembly; VfSlg 13.654/1993 regarding freedom of association.

[78] VfSlg 12.501/1990.

[79] Regarding this, cf. the amendment, BGBl I 2017/63.

IV. The right to respect of one's privacy and family life and of data protection on the Internet.

Indicator 4.1.1.

In Austria, article 8 of the ECHR, which ranks at the level of the constitution, and the fundamental right to data protection in section 1 of the Data Protection Act form the essential constitutional basis for the protection of privacy and personal data. Encroachments on these fundamental rights are permitted only under the conditions stated in article 8 paragraph 2 of the ECHR, respectively section 1 paragraph 2 of the DSG; therefore, they must be provided for under the law, must serve a legitimate goal and must be necessary in a democratic society, that is, they must be proportionate. The applicable guarantees of the Charter of Fundamental Rights of the European Union are accounted for in the enforcement of EU law (Arts. 7, 8 CFR). An overview of the corresponding basic-law regulations will be presented, which will explain these guarantees in greater detail, in the following.

1. Protection of privacy with online media

The protection of privacy is enshrined in various legislation of Austrian law. In practice, the relevant provisions on personality protection under media law are of the greatest significance, including with respect to the Internet. They bring to bear if the private sphere of a person is encroached upon by a medium within the meaning of the MedienG, meaning a 'periodic electronic medium' on the Internet, that is, a website or a recurring electronic medium.[80] They are supplemented by additional claims.

- Claims in accordance with the MedienG

The aggrieved party has the right to claim damage compensation due to violation of privacy by a publication on an online medium if either (i) the most private area of a person's life is discussed or presented in a compromising way; (ii) the identity of a person is exposed who has been the victim of a crime or is suspected of having committed a crime, respectively who was convicted of such a crime; or (iii) a publication violates the principle of presumed innocence (secs. 7, 7a, 7b MedienG). The definition of another offence protects against the publication of confidential material from surveillance by the police or the judicial authorities or from a confidential session of a parliamentary board of enquiry (sec. 7c MedienG).[81]

---

[80] Regarding these terms, cf. above, fn 22 et seqq.

[81] Regarding these offence definitions, cf. e.g. Berka, in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar* (2012) secs. 6 et seqq.

Indicator 4.1.1.

With these offence definitions, the legislature has met its duties of protection of privacy and presumed innocence as stipulated in articles 6 and 8 of the ECHR.[82]

The particulars of the offence definitions, their scope and the accompanying exclusion criteria will not be discussed in detail here. In each case, the legislature has endeavoured to carefully delineate the protected private sphere vis-à-vis the rights of the media to information that are likewise guaranteed under basic law. The consideration that the position of the affected party in public life or other contexts with public life make reporting permissible when a private context is inherently affected by this, both with respect to the protection of the most private areas of life (sec. 7 MedienG) and with respect to identity protection as per section 7a of the MedienG, is significant. The ability of the media to meet its obligation of information on public topics, including the exercise of its role as 'public watchdog', without hindrance is ensured in this way.

In the event of a violation of the offence definitions stipulated in the MedienG, the affected party has a claim to damage compensation for the injury inflicted, that is, to compensation for immaterial damage. The media owner of the relevant medium, that is, the operator of the media company, or – if publication outside of a media company is at issue – the person who, as the creator of a website or as a blogger, created the content and distributed it or caused it to be distributed, is liable. The damage compensation amounts are limited as stated above, with the upper limit amounting to €20,000.00, or €50,000.00 in cases where the publication has had a particularly severe impact.

With regard to the offences defined under media law, there is ample legal practice by the national courts up to the OGH, including, and in recent years increasingly frequent, benchmarks pertaining to the Internet. There is also applicable case law from the ECtHR, which in any case has had to revise Austrian court decisions in the past, and not just in exceptional cases, primarily when free speech and freedom of the media as per article 10 of the ECHR were not given the stipulated attention in the view of the Strasbourg court. Indeed, it must be said that balancing the opposing rights to and of information and the personality rights on a case-by-case basis is anything but simple and that the weighing of interests depends on assessments, the objectivity of which is

[82] So with respect to sec. 7b MedienG, VfSlg 14.260/1995.

often limited. Aside from that, the ECtHR has found cause less and less often in recent years to recognise a violation of the Convention in this context.

- Other defined offences against privacy protection

Indicator 4.1.1.

Along with the damage compensation circumstances already discussed, there can also be civil claims based on the right to one's own image (sec. 78 UrhG) if the publishing of a person's likeness on the Internet has a negative impact on the justified interests of the person depicted, which also include the interest in an unimpaired private life. In this case, the scope of the claim also depends on a weighing up of the opposing interests, above all the interest of the public in the relevant photojournalism.

In a similar way, a blanket clause of the Austrian General Civil Code (sec. 16 ABGB) in conjunction with article 8 of the ECHR establishes a right to anonymity that can limit the permissibility of reporting on the Internet. It protects a person from being identified by reporting and the associated exposure if this would draw the person into the public eye without justification. This also results in a weighing of interests, whereby the public's need for information is overriding if the concerned party has given an objective reason for the naming of names.[83]

2. Data protection and the Internet

In Austria, the protection of personal data depends on the European General Data Protection Regulation (GDPR), which is directly applicable, and the Data Protection Act (DSG), which, upon the coming into effect of the GDPR, applies as amended with the Data Protection Amendment Act 2018, BGBl I 2017/120.[84] These regulations apply to all Internet services and information and communication technologies for which the personal data of natural persons is processed. According to the principle of *lex loci solutionis* (art. 3 GDPR), the GDPR also applies to companies that are headquartered outside of the EU but that direct their offerings at EU citizens, e.g. Facebook or Google.

- Overview of the basic principles of data protection law

[83] For an overview and further evidence regarding these offence definitions, cf. Berka, in Berka, Heindl, Höhne and Noll, *Mediengesetz. Praxiskommentar*[3] (2012) *Vorbemerkungen* secs. 6-8a, ref. no. 10 et seqq.

[84] The GDPR and the DSG, as amended with the Data Protection Amendment Act of 2018, both come into effect on 25/05/2018. Until this date, the DSG 2000 still applies, BGBl I 1999/165, as amended, BGBl 2013/83. The representation in this text already proceeds from the new legal situation.

Within the scope of this legislation, the central principles of data protection are broadly guaranteed, and in a way that also complies with the obligations adopted by Austria in the Data Protection Convention of the CoE.[85,86] This applies, in particular, to the following principles for the processing of personal data (art. 5 GDPR):

Indicator 4.1.2.

- Lawfulness, processing in good faith, transparency: personal data must be processed in a lawful manner, according to the principle of good faith and in a way that can be comprehended by the data subject. Processing is not permitted unless there exists a specific justification cited in the GDPR (e.g. consent, legal justification, among others).
- Earmarking: data may be collected only for defined, clear and legitimate purposes. Use of the data for purposes other than those for which they were collected is prohibited on principle; however, the new law also allows for the breach of this principle under narrow preconditions.
- Data minimisation: processing must be appropriate to, and restricted to the extent necessary for, the purpose of the processing.
- Accuracy: the processed data must be objectively accurate and up to date; inaccurate data must be deleted or corrected without delay.
- Limitation of storage time: data may not be stored in a form that enables identification longer than is necessary.
- Integrity and confidentiality: data must be processed in a way that ensures appropriate security of the personal data.

Indicator 4.1.3.

Additional regulations concretise these principles; the following contexts are referenced by way of example:

Indicator 4.1.4.

- Informed consent: where the lawfulness of an instance of processing depends on the consent of the data subject, the new legal situation has strengthened the requirements (e.g. knowledgeability regarding purpose and scope of processing, comprehensibility, revocability).
- Claims to information: data subjects must be comprehensively informed regarding the nature and manner of the data processing and regarding their rights.
- Rights of data subjects: data subjects have a right to information about the processing of personal data, to the correction of inaccurate data and to the deletion of data when, among other things, it is no longer needed, consent to processing has been revoked or when a justified objection to the processing is submitted.
- Profiling: automated processing of personal data based on the assessment of personal aspects pertaining to a natural person for the analysis or prognosis of aspects concerning the job performance, economic situation, health, personal preferences or interests, reliability or behaviour, residence or change of location of the data subject is permitted only under limited conditions.

[85] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, SEV No. 108, ETS 108, BGBl 1988/317 as amended with the supplementary protocol dated 08/11/2001, BGBl III 2008/91.

[86] Regarding the legal situation in Austria with respect to data protection, cf. e.g. Knyrim (ed.), *Datenschutz-Grundverordnung* (2016); Feiler and Forgó, *EU-DSGVO* (2016).

- Data portability: The right of data subjects to receive provided data in a structured, established, machine-readable form in order to give them a different purpose is of particular significance for the Internet.

The GDPR stipulates the establishment of an independent oversight authority to monitor the data-protection regulations with the aim of protecting fundamental rights and freedoms. In Austria, this is the Data Protection Office, which on principle fulfils the required guarantees of independence. It is also equipped with the expertise required to ensure compliance with the general legal conditions for data protection.

With these and other provisions, the new Data Protection Act had updated the previous legal data protection standards and principles and incorporated them into a set of European regulations (the harmonisation of which is indeed only limited). The question of whether the challenges of the future, which become apparent in particular in connection with the way in which the Internet and other digital services (big data, cloud computing, etc.) pervade everyday life, can be overcome in this way remains doubtful and is disputed by some.

- Data protection, free speech and freedom of the media

Because data protection law gives individuals the most extensive possible right to control over their personal data and means to restrict the processing of personal data, data protection is in a tense situation with respect to free speech and freedom of the media. This has manifested itself in, for example, a current case decided by the Constitutional Court. In this case, the court repealed a regulation from the earlier DSG as unconstitutional because of an unreasonable encroachment upon the right to free expression and freedom of information that obliged the operator of a publicly available data application to delete data without making this obligation dependent upon a weighing of interests. This particular case concerned an Internet portal in which information was given about physicians practising in Austria and where users could give relevant evaluations.[87]

The European GDPR ceded the resolution of this tension area with free speech and freedom of the media to the national legislatures to a large extent. According to article 85 of the GDPR, the member states must use relevant legislation to harmonise the right to the protection of personal data with the right to free expression and freedom of information, including processing for journalistic purposes and scientific, artistic or

[87] Cf. VfSlg 20.014/2015; OGH 27/06/2016, 6 Ob 48/16a.

literary purposes. For this purpose, they may provide for deviations from and exceptions to the substantial provisions of the GDPR.

In the Austrian Data Protection Amendment Act, the national legislature is attempting to fulfil this task in the provision of section 9 DSG. Indeed, it is doubtful whether it has actually succeeded in doing so since the regulation is extremely vague in a number of respects and does not actually resolve the mentioned tension area. This means that the term 'journalistic purposes' is not more specifically defined, and it is ultimately left up to enforcement to what extent exceptions to the provisions of the GDPR are to be considered 'necessary' in the interests of free speech and freedom of information. These ambiguities are particularly problematic when it comes to publications on the Internet because, in contrast with the 'traditional mass media', journalistic activities that do not correspond to the traditional makeup of the profession of journalist, but which are nevertheless privileged with free speech, are relied upon much more frequently in this case. The scope of the exemption with regard to artistic and literary purposes is also unclear.

3. Protection of anonymity on the Internet and the use of encryption technologies

Indicator 4.1.7.

The discussion on the value, or lack thereof, of anonymous publications on the Internet has also been controversial in Austria. It can be ascertained from the perspective of the law that there does not exist any legal obligation to use a real name. The Media Act even protects anonymity, which has been viewed in the traditional media world as a condition of freedom of the media, in a particular way. The editorial confidentiality recognised under media law gives journalists the right to protect the identities of their sources and also prohibits circumvention of this right, for example, by the government seizing documentation.[88] The liability under tort law regulated in the MedienG for encroachments upon personality rights was introduced against the background that publications via the media are often made anonymously and it is therefore often impossible to tell who the actual authors of compromising pieces are; in order not to leave the data subjects unprotected, the damage compensation duty is thus imposed upon the media owner in the form of strict liability. To the extent that the regulations governing editorial confidentiality apply to journalistic activities on the Internet, this guarantee also brings to bear on publications on the Internet.

[88] Cf. above, fn 45.

However, persons who become the victims of anonymous allegations on the Internet are not unprotected. Rather, under certain conditions, based on section 18 paragraph 4 of the ECG, they are able to demand the disclosure of the name and address of a user of a service so that they can pursue their legal claims (for example, against a poster).[89]

The use of encryption technologies is not subject to any legal restrictions. However, government authorities are also meant to obtain access to encrypted Internet messages as part of the planned expansion of surveillance options.[90]

V. Government surveillance of the Internet

1. General legal conditions

Indicator 4.2.1.

The surveillance of Internet activities by government authorities is subject to strict general constitutional conditions. The constitutional legality principle (art. 18 B-VG) is to be applied to surveillance measures, meaning that the powers granted to police and judicial authorities must be regulated by sufficiently specific formal laws that stipulate the prerequisites, circumstances and procedures. The necessity of sufficiently precise and accessible legal bases can also be derived from the applicable fundamental rights. The fundamental rights to respect of one's private and family life and communication (art. 8 ECHR, art. 7 CFR), the fundamental right to data protection (sec. 1 DSG, art. 8 CFR) and constitutional telecommunications secrecy (art. 10a StGG) apply.

The corresponding powers of the police were also expanded in recent years, including in Austria. Moreover, it can be expected that further authorisations will also be granted in future for the purpose of combating terrorist activities and other forms of criminal activity, if nothing else than in view of the rapid development of communication technologies. Such surveillance measures not only affect communication by means of the Internet, but in fact they often and predominantly affect such communication. Indeed, the practices of the Austrian courts, above all the case law of the Constitutional Court, show that the surveillance of citizens by the police and law enforcement agencies is subject to strict scrutiny in accordance with legal standards, for which the aforementioned fundamental rights are also invoked. The repeal of legal provisions on

[89] Regarding the prerequisites in detail, cf. OGH 30/01/2017, 6 Ob 188/16i.
[90] Regarding this, cf. below, fn 97.

data retention by a verdict of the Constitutional Court, which could be based upon a decision obtained by the Constitutional Court from the ECJ, proves that restrictions of human rights are taken seriously.[91]

Indeed, an appropriate balance between the fundamental guaranteed freedoms, which a democratic society must not surrender, and that society's security needs, which cannot be denied in the face of increasing threats, remains an ongoing challenge. A societal discourse that includes the participation of the crucial authorities of civil society is necessary. In this respect, it is important that there be an alert public in Austria that ensures continued intense debate on the necessity and appropriateness of new surveillance measures.

2. Overview of the surveillance powers of police and judicial authorities

The most significant legal bases for scrutiny and surveillance of Internet activities can be found in the Federal Security Police Act (SPG), the Police State-protection Act (PStSG), the Code of Criminal Procedure (StPO) and the Telecommunications Act (TKG). An overview of these is presented here.

- Security police surveillance
- The SPG primarily regulates the tasks and powers of the security agencies with respect to preventative police work, that is, during the prevention and hindrance of punishable acts. In cases where Internet communication is being monitored, the law provides primarily for the following powers:[92]

Indicator 4.2.2. Indicator 4.2.3.

- Disclosure of core data: the security agencies are authorised to demand the disclosure of core data (name, address, participant number) of a particular connection (landline, mobile communications, Internet telephone) from service providers in order to fulfil their duties.
- IP disclosure: in order to defend against dangerous attacks, criminal ties or risk to the life, health or freedom of a person, the authorities may demand the disclosure of the IP address assigned to a particular message and the name (user) to which an IP address was assigned at a particular time. As a result, a message of which the authorities have already become aware can be assigned to a user of the IP address.
- Re-recording call data: authorities can demand the disclosure of the connection and the identity of a caller in order to protect against dangerous attacks and to fulfil their first general duties to provide assistance.

[91] Cf. VfSlg 19.702/2012 and VfSlg 19.892/2014 in conjunction with ECJ 08/04/2014, C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, among others.

[92] Regarding this, cf. sec. 53 para. 3a, para. 3b and para. 4 SPG; for details, Keplinger and Pühringer, *Sicherheitspolizeigesetz*[16] (2016).

- Providing a location: information on location data and the IMSI identifier of a person likely to threaten public safety or a threatened person (including companions) can be retrieved and the locations of such persons determined in order to provide assistance or protect against a threat to the life, health or freedom of a person.

These powers of the security agencies make it possible to determine the identity of a user and the user's location. Security agencies are not permitted to access the content of communication conducted using Internet services or the content of accessed websites. Practice therefore assumes that constitutional telecommunications secrecy (art. 10a StGG), which permits access only on the basis of a judicial order, is not affected by these powers.[93] Security agencies may access data available publicly on the Internet to fulfil their duties in the most general sense.

Informing the data subject regarding requests for information is not provided for by law, but a legal protection officer must be informed about the measures listed above (with the exception of the disclosure of core data) and the use of technical means by the authorities to geolocate mobile phones (sec. 91a et seqq. SPG).[94]

In order to protect against attacks that threaten constitutional rights, in particular religiously or ideologically motivated violence, the constitutional protection authorities are granted powers that are broadly similar to those listed above. However, with respect to the obligation to provide information on traffic, connection and location data, this law goes further. The measures provided for in the Police State-protection Act are likewise subject to scrutiny by legal protection officers.[95]

On principle, these powers of surveillance comply with constitutional requirements with due regard for fundamental freedoms and human rights. They are precisely regulated under the law to the greatest possible degree of certainty, they serve the legitimate goal of preventing dangerous attacks or other risks, and they stipulate the elemental prerequisites of the measures with respect to their aims, the persons under surveillance and the permitted duration of their implementation in an appropriate manner. Further handling of the data acquired, that is, storing and transmitting it and securely keeping it, is regulated in the SPG with a focus on the relevant principles under data protection law. The Data Protection Act applies to the use of personal data

[93] Regarding the constitutional-law limitations of the powers and their permissibility under constitutional law, cf. VfSlg 18.830/2009 and VfSlg 19.657/2012.
[94] Regarding the tasks of the legal protection officer, cf. below, section V.3.
[95] Cf. especially sec. 11 PStSG Regarding the constitutionality of the investigatory powers provided for in this law, cf. VfGH 30/11/2017, G 223/2016.

by the security agencies with due consideration for the principle of proportionality, provided that the SPG does not expressly mandate otherwise (sec. 51 SPG).

- Surveillance by judicial authorities

Indicator 4.2.2. Indicator 4.2.3.

The judicial authorities (public prosecutors, criminal courts) are likewise granted powers to monitor messaging traffic in order to shed light on and prosecute punishable acts as per the Criminal Code and the supplementary criminal laws. The corresponding orders are generally issued by the public prosecutors charged with conducting the investigation proceedings with the cooperation of the criminal police. In most cases, the corresponding orders require approval from a judge. In cases where Internet communication is being monitored, the law provides primarily for the following powers:[96]

- Disclosure of core data and IP: in order to shed light on criminal acts, the operators of communications services are obliged to relay the core data of a subscriber, as well as certain data from an instance of Internet communication (primarily the IP address of a specific communication, name of the user of an IP address, email address) obtained during the processing of traffic and access data, to the criminal police and judicial authorities.
- Disclosure of message transfer data: service operators are obliged to disclose traffic, access and location data accruing in the context of an electronic communications service or an information society service. This disclosure may be requested in the event that hostages are taken, for the purposes of a manhunt or to shed light on a gross criminal act (potentially carries a prison sentence of more than one year).
- Monitoring messages: the content of messages that are transmitted via electronic communications services or information society services may be monitored. However, again, a hostage situation, a manhunt or shedding light on gross criminal acts that are referred to specifically under the law are required conditions for such surveillance.

According to these provisions of the StPO, the judicial authorities can also access and monitor the content of messages, which differs from the surveillance measures of security police; this concerns, for example, email traffic, blogs or postings, VoIP, WhatsApp or Facebook Messenger. On the other hand, apart from cases of abduction or enquiry as per sec. 76a of the StPO, these measures always require approval from the competent judge; this is also required under constitutional law with respect to telecommunications secrecy and the requirement of a court order contained in this fundamental right. The understanding of the data subject after the investigation is over is also required under the law; however, obtaining this understanding can be postponed

[96] Regarding this, cf. sec. 76a and secs. 134 et seqq. StPO; for details, see Reindl-Krauskopf, Tipold and Zerbes in Fuchs and Ratz, *Wiener Kommentar StPO* sec. 76a, secs. 134 et seqq.

for as long as the purpose of this or another procedure would be threatened by doing so.

As a result, it must be assumed that authorisations to monitor Internet communication as part of a criminal trial take the requirements of the ECHR sufficiently into account. This applies with respect to their regulation through a sufficiently precise law and more detailed drafting of the prerequisites and legal consequences of surveillance that sufficiently accounts for the requirements of proportionality, primarily by restriction to gross criminal acts. The infiltration of a computer with spy software in order to obtain access to the content of messages that were encrypted for their transmission without legal backing is unlawful according to applicable Austrian law.

- Current developments

Indicator 4.2.5.

A draft of an amendment to the StPO proposed in summer 2017 proposed to create these missing prerequisites for the surveillance of messages and information that are encrypted end-to-end and that are distributed via Internet services such as Skype or WhatsApp. This authorisation was also intended to cover the installation of programs on computer systems without the user's knowledge that would be able to bypass encryption. Such an instrument is considered to be 'urgently necessary' by law enforcement agencies, not least because they are meant to be used to prevent offenders from gaining an advantage through the choice of a certain means of communication. A new version of the concept of monitoring messages was meant to further clarify that not only is the exchange of ideas between people included in the surveillance measures, but in fact all data transmission is, for example, visiting websites or making transfers in a cloud.[97]

It is clear that the use of surveillance software in order to leak encrypted messages is an encroachment upon the integrity of computer systems. Whether the associated drawbacks could be tolerated depends in particular on the additional security measures, not least on the requirement that the software used be restricted to the functions provided for under the law and that the transparency of the measures taken be ensured.

Another draft was submitted simultaneously that proposed an obligation of the operators of communications services to participate in a 'quick-freeze procedure' that is meant to take the place of data retention. According to this draft, it would be possible

[97] Cf. sec. 135a StPO according to draft 325/ME 25. GP.

to use a corresponding order from the public prosecutor to oblige operators to continue to store the traffic data for a maximum period of 12 months and to transmit it to law enforcement agencies in cases where an obligation to disclose information exists according to the provisions of the StPO.[98]

The pursuit of this draft was temporarily suspended due to the end of the legislative period and the new elections in the middle of October. However, it can be expected that the matter will be taken up again in 2018.

3. Regarding scrutiny of surveillance powers

The question of whether government surveillance measures can also be applied in specific individual cases under strict observation of the limits and conditions that arise from the applicable fundamental freedoms and human rights depends on the existing powers of scrutiny and monitoring and their use. With respect to the legal protection of users of Internet-based services who are affected by government surveillance measures, the legal bases of these measures under security police law, respectively under criminal trial law, must once again be distinguished. Furthermore, the powers of supervision granted to legal protection officers in both contexts must be discussed.

- Legal protection with respect to the surveillance powers granted to security police

Indicator 4.2.6.

On principle, the security agencies have decreed the surveillance powers as per the SPG to fall under their own area of responsibility. Judicial approval is not provided for and, according to the view of the Constitutional Court and prevailing doctrine, is also not necessary because the content of communications is not being monitored.[99] Data subjects can lodge complaints with the independent data protection authorities against the implementation of the measures by claiming a violation of their rights. The Federal Administrative Court decides on complaints against decisions of the data protection authorities (sec. 90 SPG).

The rights of data subjects to disclosure of processed data, correction of inaccurate data and deletion of data can likewise be asserted through complaints to the data protection authorities and, if necessary, through subsequent complaints to the Federal Administrative Court.

[98] Cf. sec. 99 para. 1a to 1f TKG 2003 according to draft 326/ME 25. GP.
[99] VfSlg 19.6572012.

In order to counterbalance the legal protection gaps caused by utilisation of surveillance measures, which are kept confidential vis-à-vis the data subject, the legislature has provided for the establishment of a legal protection officer (secs. 91a et seqq. SPG, sec. 14 PStSG). This legal protection officer and his/her representatives are provided with the power to expressly and autonomously determine constitutionality. S/he must be informed of the use of surveillance measures, supervises the legality of the use of these measures and must notify data subjects in the event of legal violations. If it is not possible to make such a notification because doing so contradicts the overriding public interest, then the data protection officer must lodge a complaint with the data protection authorities on behalf of the data subject (sec. 90 SPG). The legal protection officer must be permitted to view all necessary documentation and records; s/he must be granted all necessary disclosures and can supervise the implementation of the measures. Disclosure can be denied due to overriding confidentiality interests only in exceptional cases. (sec. 91d para. 1 SPG). ***Indicator 4.2.7.***

The legal protection officer is required to prepare an annual activity and performance report, which must be submitted to the Interior Minister, who must then forward it to the competent parliamentary subcommittee. Publishing this report is not stipulated, but the legal protection officer reports on his/her activity in anonymised form annually in a professional journal.[100] ***Indicator 4.2.11***

- Legal protection for surveillance measures undertaken for a criminal trial

It has already been stated that, apart from strictly defined exceptions, surveillance measures by the criminal police and public prosecutors routinely require judicial approval. ***Indicator 4.2.6.***

A claim due to violation of rights as per section 106 of the StPO can be lodged against the ordering and implementation of such surveillance measures. This must be decided on by the court. An application for renewal (sec. 363 a StPO) can be brought to the attention of the OGH when a violation of rights under the ECHR is claimed, including by affected third parties who can assert a claim that their fundamental rights have been violated.

[100] Cf. most recently Burgstaller and Kubarth, *Zentrale Daten des RSB für 2015*, SIAK Journal 3/2016, 4; Burgstaller, Goliasch and Kubarth, *Zentrale Daten des RSB für 2016*, SIAK Journal (in press).

There is also an autonomous legal protection officer in the judicial sector. This officer's responsibilities are limited in the existing context, that is, with respect to the supervision of Internet-based communication, to the review and scrutiny of measures that encroach upon the rights of persons who have the right to professional secrecy (sec. 147 StPO).

- Supplementary remarks

Indicators 4.2.6.-4.2.10.

In summary, it must be restated that encroachments upon the rights of data subjects in the context of Internet communication are subject to scrutiny by independent courts, so, by either the administrative courts or the regular courts. Guaranteeing legal protection can pose difficulties if the measures must be kept secret vis-à-vis data subjects in order to avoid threatening the purpose of the investigation. This applies primarily to measures under the SPG for which subsequent notification by the authorities is not stipulated. By establishing legal protection officers, the legislature has attempted to counteract this legal protection gap and grant 'provisional legal protection'. It is attested that this solution has proved successful on principle, even if there is criticism of the powers of scrutiny and oversight available to the legal protection officer and there is a question as to whether the legal protection officer still has sufficient capacity to fulfil his/her duties to the stipulated degree of thoroughness in light of the expansion of police surveillance measures.

Scrutiny from the perspective of protecting fundamental freedoms and human rights is ensured as part of judicial powers and surveillance by the legal protection officers; observing these freedoms and rights is part of the task of monitoring legality with which these bodies are entrusted.

Furthermore, powers of scrutiny and oversight are granted to the data protection authorities when data is used by security agencies.

Indicator 4.2.11.

With regard to informing the public about the activities of offices that implement surveillance measures, the legal situation in Austria complies with the requirements of transparent, open public administration only to a limited extent. The same applies to notifications via the bodies that scrutinise and oversee these measures. Indeed, the administrative authorities are bound by a disclosure duty that is enshrined in the

constitution, but it is structured in such a way as to be inexpedient. First and foremost, there is criticism of the fact that official secrecy ranks at the level of the constitution (art. 20 paras. 3, 4 B-VG) and that the appeal to administrative duties of secrecy plays a significant role in practice. The passage of a constitutional freedom of information law has been advised for a considerable time; a draft of such a bill has existed since 2014. It would require the aforementioned institutions to actively inform the public about their activities and, at the same time, grant citizens a fundamental right of access to information, which would, on principle, also relate to the activities of the surveillance authorities and their supervisory bodies. The fate of this draft is still open at the time of writing.[101]

VI. Legal remedies

- Access to judicial legal protection

Indicator 5.1.

Access to the courts is broadly guaranteed under Austrian law and also practically feasible. This also applies to all branches of jurisdiction, so, to civil jurisdiction, criminal jurisdiction and public-law jurisdiction (administrative- and constitutional-courts jurisdiction). Judicial independence is guaranteed in the constitution and ensured in actuality.

The procedural law of the courts meets the principles of article 6 of the ECHR and the requirements of fair proceedings are also accommodated in individual cases. In this way it is guaranteed on principle that alleged human-rights violations committed online are decided upon in fair, public proceedings and within an appropriate period of time by an independent, impartial court.

Since 2014, a wide-reaching reform of the administrative court jurisdiction has ensured that even encroachments by police or other administrative authorities are subject to scrutiny by the administrative courts, which are equipped with broad powers of cognition, that complies to its full extent with the European standards specified by the ECHR and EU law.

Due to the design of the legal protection, which clearly focusses on formal types of action by the administration, there can be certain legal protection gaps in the area of

[101] Cf. draft 395 Blg no., 25. GP, which admittedly became irrelevant upon expiry of the last legislative period and which provided for relevant constitutional modifications. Regarding this draft, a supplementary draft of a freedom of information law was submitted in the constitutional committee.

informal administrative action or with respect to official failure. However, it is not apparent that this results in problems in the contexts of online activities that are of interest for the purpose of this report. In any case, this is conducive to the possibility of combating even atypical, informal administrative action in the area of police law by complaining to the administrative court (sec. 88 para. 2 SPG).

- Other legal remedies

Indicator 5.2.

The requirement of an effective right to complain within the meaning of article 13 of the ECHR is complied with based on the broad judicial responsibilities. The direct applicability of the ECHR and its application as part of Austrian federal constitutional law ensures that the guarantee of legal protection by the courts also includes the fundamental freedoms and human rights of the Convention.

The guarantee of 'provisional legal protection' by the independent legal protection officers that exists in the area of the judiciary and that of the security police has already been discussed.[102] They are of particular significance for the scrutiny of confidential surveillance measures, even and especially with respect to the surveillance of Internet activities. In this way, as part of their options, they contribute to the factual and effective guarantee of legal protection in this sensitive area.

Finally, the responsibilities of the Ombudsman Board must also be mentioned (arts. 148a et seqq. B-VG). This independent supervisory body can be invoked due to any claimed grievance in the administration of the federal government; the Ombudsman Board is assigned the task of protecting human rights in special way. This option to lodge a complaint, which can be utilised informally and without cost barriers, is also available in connection with the surveillance powers of security agencies. If a complaint is justified, the Ombudsman Board can work towards the rectification of the grievance in the form of a recommendation. The Ombudsman Board is supported by a human rights adviser and commissions in fulfilling its tasks in the area of human rights protection.[103] The Ombudsman Board is also empowered to review grievances with administration, including violations of human rights by the official authorities.

- Legal protection for private stakeholders

[102] It should only be noted that there is also an independent legal protection officer as per the Act on the Powers of the Armed Forces who is responsible for the scrutiny of the military intelligence services, and there is a legal protection officer under criminal financial law.

[103] Regarding this, cf. secs. 11 et seqq. Ombudsman Board Act 1982 BGBl 1982/433, as amended.

Indicator 5.3.

If private companies and other private stakeholders that are able to influence the realisation of the fundamental freedoms and human rights on and through the Internet are subject to legal obligation, then affected parties have the option of taking legal action in the courts. Even if private legal enforcement can be difficult and costly in some circumstances, there are no noticeable significant deficits. These proceedings also comply on principle with the guarantees of article 6 of the ECHR.

Due to the international interconnectivity of the Internet, the fact that cases often involve foreign countries means that enforcement of claims or prosecution of criminal acts can certainly result in significant problems. Difficult legal questions are posed when judicial competence for international legal issues and applicable law are determined, but there are also practical problems with legal enforcement vis-à-vis cases where legal adversaries are difficult to discern. Due to this de-territorialisation of communications law, national legislation comes up against clear limitations that can only be overcome by international legislation. A national report can only touch upon these problems.

Indicator 5.4.

If activity on social networks or other Internet platforms has an unlawful negative impact on human rights and fundamental freedoms, judicial legal protection is likewise available. However, the fact that the responsibility of intermediaries is limited, primarily by the limited liability of providers, has already been highlighted.[104] It is primarily due to the difficulties of legal enforcement that more contact points have been created in recent years to give people whose rights have been impacted or who would like to take action against illegal content on the Internet the option to lodge complaints outside of the judicial legal protection. They can advise the concerned parties and review options for legal enforcement, including in connection with government offices. The most significant institutions of this kind that exist in Austria are referred to here:

- Reporting office for child pornography: established by the Ministry of the Interior; accepts reports of texts or images that contain child pornography;[105]
- Reporting office for re-engagement in National Socialist activities: established by the Ministry of the Interior; accepts reports of websites or news-group postings with neo-Nazi, racist and anti-Semitic content; [106]

[104] Cf. above, fn 32 and fn 36.
[105] meldestelle@interpol.at; also http://www.bmi.gv.at/cms/BK/meldestellen/kinder/start.aspx (accessed on 28/09/2017).

- Reporting office for hate posting: initiated by the Office of the Federal Chancellor and operated by a private association (ZARA - Civil Courage and Anti-racism Work);[107]
- Stopline: established by ISPA (Internet Service Providers Austria); accepts reports of Nazi or child-pornography content; member of INHOPE, a network of hotlines against illegal content on the Internet.[108]

[106] ns-meldestelle@bvt.gv.at; also http://www.bmi.gv.at/cms/bmi_verfassungsschutz/meldestelle/ (accessed on 28/09/2017).

[107] https://Beratungsstelle.counteract.or.at (accessed on 28/09/2017).

[108] https://www.stopline.at/home/ (accessed on ■).

C. Communication studies analysis[109]

As with the previous treatment of the general legal framework for the implementation of Internet freedom in Austria, the communication studies discussion also focuses on the issues and indicators in Recommendation CM/Rec(2016)5 of the Council of Europe. The experiences of civil society with the utilisation of Internet freedom in Austria will likewise be emphasised along with the state of the applicable scientific research. The latter will be limited to an overview of aspects that have not already been discussed in the legal analysis.

A two-step procedure has been selected for the method of the investigation. The research team has developed an online survey from the inspection and analysis of the applicable specialised literature in conjunction with the indicators of the European Council's Recommendation; this survey was administered to representatives from civil society in summer 2017. The respondents gave their consent to their answers being quoted either directly or indirectly in the research report. Some individuals preferred to give written answers to questions rather than participate in an oral conversation.

The stakeholders from civil society that were invited to answer the questions were selected, on the one hand, based on the applicable specialised literature, and on the other by an analysis of member lists from associations and consortia (such as the *Internet Governance Forum*) and based on recommendations from persons already selected (snowball sampling). To this were added experts from academic and administrative fields. The resulting list included 58 individuals and organisations, of which precisely half (29) participated in the survey either in writing or orally (persons recorded in the appendix). We give our deepest thanks to all of the participants!

In total, five thematic groups were formed: Internet activists in a broad sense, Internet service providers, data protection experts, media representatives and academic experts. Each group received one of the indicators of the Council of Europe's Recommendation and the survey, which was tailored to the field of competence of the person or organisation.

The answers received (recorded in writing and in interview transcripts) were then assigned the topics of freedom of access and freedom of expression on the Internet,

[109] Jana Büchner and Roland Holzinger contributed significantly to the author's work on this part of the report.

data protection and the private sphere, and actual accessibility and reproduced in the report verbatim, as excerpts or in paraphrase.

The following report is thus based, on the one hand, on the workup of the specialist scientific literature and on the statements of the respondents, on the other. The findings will also be reproduced in this order. In contrast with the legal analysis in the first part of this report, the communication studies analysis does not make any claim to completeness of the topics considered in the Recommendation of the Council of Europe, but rather it focuses on critical aspects of Internet freedom from the perspective of civil-society stakeholders.

I. Freedom of access on the Internet

1. Introduction

Freedom of expression and freedom of access to information are two inextricable principles of free speech. Political and social participation in democracies depend on access to a large range of information and knowledge.

Networked digital technologies and, above all, the Internet are essential components of the economy, politics and everyday life in the modern world. Access to the Internet not only enables the exercise of free speech and freedom of information, but it also emphasises the state and development of a digital society, democracy and economics (cf. UNESCO 2015, 13 et seq.). Access to the technical infrastructure and access to online information form two fundamental dimensions of challenges for and limitations of freedom of Internet access (UN General Assembly 2011, 1).

The social-science concept of the ‘digital divide’ takes access to the technical infrastructure as a starting point for deliberations on the Internet as an instrument of social participation for disadvantaged groups and expands the perspective to general educational and media-competence issues, cultural and linguistic variety and the digital preservation of traditional knowledge (cf. UNESCO 2015, 29 et seq., UN General Assembly 2011, 16 et seq.). One such broad viewpoint is also manifested in the discussion on enshrining ‘freedom of connection’ in the fundamental rights (Dutton et al. 2015, 22).

The right of access to online information forms the democratic policy basis of the opinion formation process of digitally networked citizens.

The sense of ‘freedom of information’ thus includes issues of the claim to transparency of public institutions based on the potential of the Internet for effective organisation and the provision of digital data (Dutton et al. 2015, 23) and likewise the determination of its limits through, for example, data protection or national security. The problems of regulating online content that is illegal or undesirable for the community and issues surrounding the proportionality of such measures are considered to be particularly sensitive. The debate on the responsibility and liability of intermediaries and ISPs is closely linked with this. Restrictions of free access to online content by private commercial interests currently rank alongside issues of net neutrality and the enforcement of intellectual property rights, and there are also discussions of the restriction resulting from (non-transparent) selection via algorithms on online services. Cyber-attacks are also perceived to be a threat to the digital public (UN General Assembly 2011, 8-16).

1.1 Freedom of information

Access to public and government information represents a central aspect of the right to information. Such access enables the informed and autonomous exercise of civil rights and responsibilities. Conversely, the data generated, collected and administered during the performance of government and public tasks do not serve any end in and of themselves as the basis of a democratic government, but rather they serve the use of the community (cf. Yannoukakou and Araka 2014, 332, 334; Dutton et al. 2015, 23). The incorporation of the Internet into government and administrative processes (‘e-government’) not only promises a more efficient design of internal processes and the provision of personalised services, but also expands the options for granting citizens access to public information (Yannoukakou and Araka 2014, 334). ‘Open government’, which is driven primarily by the use of modern information and communications technologies, therefore represents open, transparent and thus more responsible forms of governance and administration, at the centre of which stands the right of access to public information (‘open government data’). The free and simple access to public data is associated with hopes not only of improved democratic participation, but also potential social development and economic innovations[110]. Public data may represent a

[110] The significance of continued open use of information of the public sector for modern societies and economies is addressed by the EU in Directive 2013/37/EU (cf. Yannoukakou and Araka 2014 334, European Parliament and Council of the European Union 2013).

‘sound and reliable’ basis for new products and services in this way (cf. Afful-Dadzie and Afful-Dadzie 2017, 665; Yannoukakou and Araka 2014, 333).

The protection of the private sphere represents a barrier to access to public data. This gives rise to concerns regarding the condensation of broad big-data analyses into targeted user profiles, including those based on public data (Cannataci et al. 2016, 95).

Keeping the data of government authorities confidential is often justified by the preservation of ‘national security interests’ (Dutton et al. 2015, 50 et seq.). This secrecy is limited by the proportionality of the transparency limitations vis-à-vis the interests of citizens in the information. Global disclosure of comprehensive government surveillance measures makes this a sensitive topic (UNESCO 2015, 44). In modern societies and democracies, which are essentially dependent on the availability and exchange of (digital) information, there is a broad public interest in access to the information of the public sector. The community’s appreciation for government secrecy and confidentiality is decreasing.

1.2 The responsibility and liability of intermediaries and ISPs

At the centre of the Internet stand services and platforms that convey the online communications of third parties and thus form the first instance that enables the various forms of expression. Intermediaries simultaneously represent essential ‘gatekeepers’ of the distribution of these forms of expression. Intermediaries and ISPs are therefore the point of public and political focus in their democratic and social role and the resulting responsibility in questions of how to handle online content that is illegal or considered problematic. (cf. MacKinnon et al. 2015, 7, 15).

The debate is conducted between two sides; on the one side is the perspective that ISPs and intermediaries, as media companies, are subject to the applicable regulations for media, and that they therefore carry an editorial responsibility for their services. The other position classifies ISPs and intermediaries as the technological infrastructure for online communication between mostly anonymous third parties. In practice, a system of limited liability has been established alongside ‘knowledge and control’ in the event of unlawful content (cf. Akdeniz 2016, 46).

Concerns are expressed in the literature when Internet platforms act excessively against content in order to avoid legal liability (cf. Akdeniz 2016 47; UNESCO 2015, 42). A negative dynamic of self-censorship (a ‘chilling effect’) could act against free speech in

this way. In order to prevent disproportionate limitations of free speech, such self-regulation measures of online content must comply with the principles of transparency, legitimacy and proportionality (cf. MacKinnon et al. 2015, 15; UNESCO 2015, 42).

1.3 Intellectual property and copyrights

Everyday activities in digital environments, such as retrieving information, communicating with other persons or entertaining oneself have increased the probability of coming into contact with copyright-protected material in the process. The nature and type of contact with copyright-protected content has changed with advances in digital technologies. The increased options of the Internet allow users to produce and distribute an increased quantity of content. Such content-generating behaviour often involves copyright-protected material. The current area of tension between free speech and intellectual property rights becomes clear when the focus on infringement by downloading content in violation of copyright law expands to include the use of copyright-protected materials in user-generated online content. However, such content represents a significant mode of expressing (political) opinions and access to and participation in information and knowledge in modern democracies and societies (cf. Birnhack 2003, 234 et seq.; Henningsson 2012, 23 et seq. according to Lee 2015, 33).

Since free speech is also considered a prerequisite for further human rights (e.g. the right to education, cf. Lee 2015, 220 et seqq.; UN General Assembly 2011, 7), conflicts over intellectual property rights and copyrights pose some serious challenges for digital societies (Shugurova and Shuguro 2016, 148). Transparent, legitimate and proportionate rights of copyright owners can limit free speech in the process. However, they can also contribute to the pluralism of information when the guarantee of copyrights represents an instigation to produce content (cf. UNESCO 2015, 42).

1.4 Filter bubbles and algorithms

The Internet as a communications infrastructure offers space for an enormous multitude and variety of online content that is distributed in real time in an incessant flow of information. It is predominantly private commercial online services and platforms that have been responsible for the reduction of the resulting complexity on the significant interfaces using specific algorithms as a part of their business models. Algorithms thus offer users a structured array of information, mostly as a function of individual and

interlinked online behaviour. By filtering and rearranging online content according to specific criteria, the algorithms of Internet companies have become central ‘information gatekeepers’ in digital societies (Mayerhofer 2017, 78).

For this reason, they are considered to be an important enabler of free speech on the Internet. In a digital information environment that can no longer be grasped by individual citizens, the selection work performed by algorithms achieves an access to online content that is available to all and meaningful for individuals. From this fundamental perspective, algorithm-driven online services make an essential contribution to a situation where free speech can actually be utilised on the Internet (cf. Mayerhofer 2017, 78 et seq.).

On the other hand, in the context of the increasing contribution of online content to the shaping of public opinion (cf. Gadringer et al. 2016, 2017), the selection function of algorithms is associated with significant restrictions of free access to information on the Internet. They ultimately decide which information is given priority when displayed for users and therefore which information they are aware of. Within an algorithm-generated ‘filter bubble’, users receive personalised online content in line with their own online behaviour, their own location, their own contacts, etc. (cf. Pariser 2012, 10 et seq.). This is meant to achieve better usability for users. At the same time, the selection of content serves the commercial business model of marketing individually tailored products or advertising to customers. Inside of the filter bubbles that are created by the homogeneous display of content, whatever already corresponds with the specific ideas of users is reproduced, which reinforces individuals’ own opinions (cf. Thies 2017, 102). In this way, algorithms contribute to restricting the pluralism of the Internet to a continuous confirmation of one’s own perspective (cf. Mayerhofer 2017, 79; UNESCO 2015, 46).

Filter bubbles become echo chambers through likes, shares and comments (cf. Froitzheim 2017, 106). As was feared, people who think alike meet one another in such echo chambers, which isolates them from other opinions and points of view (cf. Thiel 2017, 102). It is also insignificant for the algorithm-driven selection and prioritisation of content that relies upon the behaviour of users whether or not the information is correct (true) (on this, see also ch. II.1.3 and ch. II.2.3).

In this respect, the intransparency of the parameters by which the gate-keeping of displayed information is performed is considered particularly critical. Their effect on individuals, as well as the societal consequences, are not accessible for any individually competent use, any public discourse or any political or legal responsibility. The enormous market power of dominant platforms and services further constricts the spectrum of opinions. In view of the interests and value judgments that are reflected in the selection decisions of algorithms, which are in no way objective, this results in concerns over severe, demonstrable manipulation of opinions (cf. Mayerhofer 2017, 80; UNESCO 2015, 46).

The commercial interests of the platforms and services in loading advertising that is personalised through algorithms seem obvious. Attempts at manipulation of strategic political communication by stakeholders that knowingly polarise and control political debates using expertise on algorithms and in line with their own prognostic big-data analyses with the aid of innovative instruments (social bots, trolls) are considered increasingly alarming (cf. Harsin 2015, 329 et seqq.). The consequences of these innovative instruments of strategic political communication on the formation of opinions are still largely unclear (cf. Ferrara 2015, 2).

1.5 Net neutrality

The right of access to information and knowledge on the Internet is closely linked with the principle of net neutrality in digital society. The fundamental equal treatment of all data traffic between sender and recipient is viewed as the core of the original idea of the Internet and subsequently as a basic requirement for the development of its potential. Only an infrastructure that transports data packets regardless of their source and destination, the devices or applications used, or the nature of the content can guarantee the greatest possible access to Internet content.

Therefore, net neutrality is geared mainly toward network and Internet service providers (network providers and ISPs) with the demand for a guarantee of discrimination-free data traffic within their services (cf. Akdeniz 2016, 20; Korff and Brown 2013, 4).

Increasing commercial interests in the exploitation of Internet data traffic by network and Internet services are currently viewed as a threat to net neutrality. The introduction of specific costs for various levels of access promises new possibilities for business and

profits. If data is not provided without discrimination, it is feared that this will create a fractured Internet (Dutton et al. 2015, 65; Korff and Brown 2013).

However, the principle of net neutrality also experiences some pressure due to the distribution of content that is unlawful or considered undesirable. The management of total data traffic with filters, blocking or the treatment of such content with discrimination by ISPs is associated with legitimate social purposes, but these purposes adversely affect the fundamental equal treatment of content and data packets. Public debate that determines 'good' and 'bad' discrimination and is located within an appropriate constitutional framework in accordance with fair Internet access is integral here (cf. Akdeniz 2016 26; Dutton et al. 2015, 65).

1.6 Cyber-attacks

Restrictions of access to online content can also be traced back to cyber-attacks. At the centre of this stands 'distributed denial of service' (DDoS) attacks, which overload a web service with a multitude of search queries, rendering the affected websites temporarily inaccessible (cf. Dutton et al. 2015, 37; UN General Assembly 2011, 14). Attempts by strategically emerging stakeholders to influence the public through the use of false domains, accounts or information are also increasingly judged to be cyber-attacks on free speech that should be taken seriously. Cyber-attacks that may be traced to the government are considered to be especially critical. The use of appropriate and effective means to hold the perpetrators of cyber-attacks accountable is derived from its obligation to protect the free speech of its citizens from interference by third parties (cf. UNESCO 2015, 43; UN General Assembly 2011, 15).

2. The results of the expert survey

2.1 Legal framework

There is an overwhelming consensus among the experts that the Austrian legal framework does not disproportionately restrict freedom of access to and freedom of expression on the Internet. While the criminal-law framework is judged to be appropriate, there are concerns regarding the legal framework for free access to public information (official secrecy).

2.1.1 Regulation of online content that is criminally relevant

The experts from academia, civil society and the digital economy view the existing regulations on media-content offences on the Internet as sufficient. They stress the importance of the judgment of criminally relevant content by courts (e.g. incitement, cyber-bullying, defamation, slander, abuse). It is difficult to determine what constitutes 'damaging, undesirable or offensive' online content, which is particularly relevant when it comes the phenomena of hate speech and 'fake news'.

Some respondents locate a weakness in the implementation of measures that have been ordered by a court. There is hardly any functional equivalent on the Internet to the traditional opposing point of view, sequestration and confiscation.

Even if the existing criminal-law framework is considered to be well-suited to the challenges of online communication, according to criminal-law experts from the Austrian Federal Ministry of Justice (BMJ), current developments, particularly those in social media, require adjustments to the legal situation. The representatives of the Democracy Centre Vienna view the newly introduced criminal offence of 'cyber-bullying' (sec. 107c StGB) into the criminal code and the amendment of the criminal offence of 'incitement' (sec. 283 StGB) as improvements to the legal situation. Because the provisions have only been in effect for a short time, the 'general deterrence effect' cannot yet be assessed. However, in the opinion of the representatives of ISPA, the adoption of new special criminal offence definitions covering wrongful acts on the Internet should be feasibly avoided.

2.1.2 Official secrecy and a freedom of information act

The overwhelming majority of experts note an urgent backlog of requests for information disclosure and access to public information. Most notably, the respondents criticise the lacking transparency of policy and administration due to the continued existence of statutory official secrecy, which has constitutional status and is considered to be anachronistic, and the lack of a freedom of information law. The 'global right to information rating', in which Austria has ranked in last place for seven years (cf. Access Info Europe & Centre for Law and Democracy 2016), has been called to mind multiple times. According to one of the experts, the repeated tabling of a submitted freedom of information law is a stalling tactic by the government. In the opinion of one scientist from the University of Salzburg, the prevailing information culture in public

institutions remains based on demand. Even if general availability and usability of public data is not guaranteed in Austria, according to the experts at ISPA, the federal 'Open Data' portal (data.gv.at) represents an example of good practice and a starting point for further efforts.

At the same time, according to the opinion of a computer scientist who was surveyed, there is still little clarity regarding measures required for the general availability of public data that accompany measures to protect the privacy of citizens with anonymisation and pseudonymisation.

The experts of ISPA characterise the work of the legal protection officer [*Rechtsschutzbeauftragter*, RSB] on security police surveillance measures as 'consistently positive and efficient legal protection'. However, non-public activity reports would contradict the transparency of government activity. This criticism can be rebutted with a reference to the annual publication of the 'Core Data of the RSB' in the journal for police science and police practice (SIAK Journal, cf. most recently Burgstaller and Kubarth 2016), which was initiated by the RSB.

In this context, the experts on the digital economy emphasise the commitment of Austrian ISPs to disclose any restrictions of the rights of users, e.g. the blocking of websites.

2.2 Case law

Several experts gave a reminder that only courts can judge the unlawfulness of statements of opinions. Their decisions should enable a clear differentiation between unlawful online content and undesired but still tolerable online content. The representatives from the media sector, academia and the digital economy attest that the weighing of interests in case law represents a good balance of the various fundamental rights claims.

Court verdicts on unlawful content and their authors draw the limits for statements of opinion online and contribute to the formation of a public consciousness. A signal effect developed due to the court proceedings of the former spokeswoman for the Austrian Green Party, Eva Glawischnig-Piesczek, against a defamatory hate post on Facebook. Criminally relevant statements have been observed with greater frequency in Austria since the wave of migration in 2015/2016. Penal action has increasingly

been taken against hate speech or ‘cyber-bullying’, including in youth environments (schools, educational institutions). According to criminal-law experts of the BMJ, court verdicts would increasingly have a deterrent public image for potential offenders.
The representative of the Chaos Computer Club Vienna (C3W) indicates that comparatively few lawsuits are brought by private persons vis-à-vis authors of defamatory or libellous online content in Austria. This fact is due less to such offences being seldom committed than to the great obstacles that victims themselves must clear before the court.

Moreover, the importance of awareness-raising measures by all of the stakeholders participating in the Internet in addition to the legal path is stressed. A variety of initiatives are meant to facilitate a tolerant and respectful culture of discussion as an important component of media competence (e.g. Saferinternet.at, ‘Chaos macht Schule’ [Chaos is catching on], the ‘Trusted Flagger’ programme).
Concerns have been expressed on the civil-society side by epicenter.works regarding the criminalisation of statements of opinion, including online, due to the penalisation of ‘subversive movements’ (sec. 246a StGB). However, since this provision only took effect on 01/09/2017, its impact cannot yet be judged.
Caution is generally required when the legal prosecution of unlawful content also includes ISPs. This could quickly lead to a ‘chilling effect’ on free expression on the Internet.

2.3 Prosecution

If presumed criminally relevant content is discovered on the Internet, it can be shown to a range of reporting and contact offices, for example, the Cybercrime reporting office, the reporting office for criminally relevant content in the area of child pornography (Federal Ministry for Internal Affairs), Stopline (an initiative of Internet Service Providers Austria [ISPA] for criminally relevant content in the area of re-engagement in National Socialist activities and child pornography) or the Internet Ombudsman for Internet fraud, especially in the area of electronic commerce. The respondents view this notification system as a positive example of cooperation between civil society, the state and the digital economy.

They also rate the initiatives against unlawful and offensive content on the Internet (in particular the establishment of the #GegenHassimNetz [#againsthateonthenet] advice

centre) in combination with the hope of an EU-wide regulation for the purpose of a 'notice and fair-balance procedure' as positive.

As well as the administrative processes function in the reporting offices, the experts from academia, civil society and the digital economy see a potential for improvement in the efficiency and pace of the cooperation between the participating stakeholders and in the quantity and expertise of the investigation personnel. The ISPA experts describe obstacles to the communication between platform operators and security agencies, for example due to uncertainty regarding the correct form of reporting (e.g. unique URL or screenshot) or when contact is made (e.g. via a contact address or an available single point of contact).

Experts from the C3W, the Digital Society and the Austrian Institute for Applied Telecommunications (ÖIAT) explicitly criticise the fact that, firstly, slander, cyber-bullying and identity theft can currently only be reported at police departments and, secondly, that the police lack the appropriate specialists to process these reports.

The experts from the Digital Society currently also see the prosecution of unlawful content outside of Austrian national territory and the EU as a significant challenge. Due to the internal processes of the authorities, international cooperation between law enforcement agencies via the Mutual Legal Assistance Treaty (MLAT) is time-intensive and therefore minimally effective.

In summary, the experts from academia, civil society and the digital economy tend to find that government institutions are overextended in dealing with the expanded options for free expression on the Internet.

2.4 Assessment of online content by private operators

ISPs and intermediaries in Austria must act against online content at the order of constitutional (judicial/administrative) authorities, for example, against illegal (child pornography, re-engagement in National Socialist activities) and criminally relevant (incitement, cyber-bullying, defamation, slander, abuse) content. According to experts from academia and civil society, content that infringes copyright law causes problems. The legal basis and practice when rights-holders demand that internet access operators block websites with content that infringes copyright law, including without a relevant constitutional decision, are unclear.

Further-reaching activities of the ISPs are viewed very critically by the experts. For example, the expert from the C3W judged any unilateral restriction of content by platform and access operators to be a restriction of free speech. The actual restriction of online content is criticised less by the experts; rather, they focus on the justification, transparency and procedure of such restriction.

According to estimates of the representative of the VÖZ and the Digital Society, the various measures that apply to international platform companies and those under Austrian law result in a paradoxical practice of removal. In this context, multiple experts have criticised the practice of removal, as well as how Facebook reports are handled in Austria. With respect to the temporary suspension of the Facebook account of writer Stefanie Sargnagel, the C3W indicates that this can also develop a dimension of free speech restriction in Austria. The removal of content from internal departments or even broadcasting algorithms without constitutional bases is considered particularly alarming.

There is general agreement among the experts that content regulation overwhelmingly represents a government task that is the subject of a judicial or quasi-judicial weighing of interests. However, private access and platform operators would fall under public responsibility to the extent that they voluntarily cooperate with government institutions and civil-society initiatives to prevent the distribution of unlawful content via their services.

The criminal-law experts of the BMJ emphasise the significance of civil-society and individual initiatives, in addition to covering and avoiding regulatory grey areas for hate speech, rumours and false reports in private initiatives (e.g. child protection filters for private Internet connections).

However, the representatives of the digital economy and civil society indicate that the public pressure on ISPs to quickly resolve the problem of prohibited content by removing it could overshoot the mark. This is specifically the case if ISPs also remove or block unpopular but legitimate content in the same accelerated procedure.

2.5 Access restrictions due to copyrights and patents

Copyright infringements currently represent the only legally permissible justification for blocking in Austria. Experts on the digital economy, as well as those from academia and civil society, criticise the fact that, due to the current legal situation, access

operators are put into a position where they have to independently balance ownership rights and free speech and are liable for unjustified blocking. If an Internet operator receives a demand from a rights-holder, the operator can only restrict free speech by blocking the content or bring about a judicial decision, thereby accepting the associated risk of the lawsuit cost.

ISPA also expresses concerns vis-à-vis the simultaneous blocking of a variety of websites with so-called IP blocks sought by the rights-holders.

The risk of 'over-blocking', which also threatens to block websites with legally compliant content, is associated with this. A structured procedure and an independent institution with the necessary competence are lacking here. Without these, oversight of the blocked websites and the statutory violations that cause the blocking is currently lacking. Because these blocks are not regularly reviewed later, under current legal practice, affected websites remain inaccessible for an indefinite time ('blocked website graveyard').

From the perspective of the rights-holder, the representative of the Association of Austrian Commercial Broadcasters (VÖP) speaks of insufficient protection of copyrights and licence rights in the existing legal framework. The Electronic Commerce Act releases access and platform operators, as 'host providers', from any responsibility for legal violations within their services. They therefore have no incentive to prevent copyright infringements of their own accord, e.g. by pre-checking the content with appropriate technical measures or by blocking repeat offenders. The protection of copyrights ultimately also serves (Austrian) content production and variety.

The expert from the Austrian Chamber of Labour Vienna absolutely recognises the dilemma of a need for greater law enforcement for rights-holders. However, the constitutional framework and corresponding guarantees of legal protection must be essential criteria for any measures.

The experts from the University of Salzburg and the World Information Institute/Institute for New Cultural Technologies perceive academics and the educational system to be generally handicapped with the expansion of patents and copyrights. Patents would restrict access to research results and make it impossible to use 'open educational resources'. The expert from the C3W says that software patents

of predominantly larger companies work against an open Internet in that they represent indirect barriers (to market entry).

2.6 Filter bubbles and algorithms

The respondents view the use of algorithms and the creation of filter bubbles as potential threats to free speech. The representative of the VÖZ sees these as causing an erosion of the process of opinion formation. He argues that traditional media provide a representation of a diverse spectrum of topics and opinions and weight the topics as part of a system of editorial checks and balances. Due to a '*limitation to few (and specific) sources of information that are no longer characterised by quality-controlled journalism, but rather by deliberate cultivation of outrage [and] propaganda*' (a representative of the ORF), outside-the-box thinking is lacking, for one thing, and a risk to the politics of democracy is created, for another. The representatives of the VÖP also see the pre-selection mechanisms as contradictory to the goal of creating and ensuring a diversity of opinions and media. Due to the personalisation of content, the expert from the C3W deems an objective representation of information to be impossible if this is not comprehensively clarified for citizens.

According to the experts from academia and epicenter.works, the effects of algorithms and filter bubbles on the debate for the 2016 presidential election were perceptible. However, the extent of their influence at the level of democratic policymaking cannot currently be estimated. In the opinion of the VÖZ representative, even now measures must be taken to oppose long-term effects that could emerge only after five to seven years.

Experts from civil society, academia and the media noted that the filter-bubble effect that is of concern for democratic policymaking is the expression of a perhaps thoughtless, but in any case voluntary, exploitation of the media. This means that more efforts to expand awareness-raising media competence are necessary.

Internet filter bubbles impact not only how the recipients form opinions, but also the quality of traditional media. The algorithm-driven options for reaching target groups in a way that perfectly suits them are increasingly directing advertising expenditures towards the large Internet platforms and less and less to the journalistic media. The representative of the VÖZ says that this is causing losses in income, resulting in attempts to save money on editorial staff, which in turn negatively impacts quality. In

this way, algorithms and large Internet platforms' focus on target groups have an indirect influence on opinion formation.

2.7 Net neutrality

The experts describe universal net neutrality as an important condition and part of the infrastructure (epicenter.works) for ensuring free speech on the Internet. In the opinion of the VÖP expert and the experts from nic.at, because network operators are prevented from discriminating between content in data transport, net neutrality indirectly serves free speech. However, net neutrality is only *one* component for ensuring free speech.

The state of net neutrality in Austria is judged differently by different experts.

An overwhelming proportion of academic experts and those from the technology sector, the digital economy and parts of civil society characterise net neutrality as 'well regulated', with reservations (nic.at), and 'guaranteed'. With reference to the 2017 net neutrality report by the RTR GmbH company, '*in Austria, there is currently no threat to net neutrality*' (ISPA). According to scholars from the Institute of Technology Assessment (ITA), ISPA represents a lobby in Austria that takes net neutrality seriously. The representatives from nic.at and the Digital Society classify repeated attempts by individual telecommunications operators to give preference to their own products as not currently a relevant problem for Internet freedom. Certain measures taken by Internet providers to manage data streams are in the interests of customers, but binding rules for providers for the purpose of standardisation were lacking.

This is where the criticism comes in. Civil-society experts (C3W, epicenter.works) view attempts by major mobile operators to prioritise data as an indication that net neutrality is being undermined in Austria. However, due to lacking measurement data and transparency of filter and prioritisation measures by the network operators, it is difficult to assess the situation. RTR GmbH would exercise only insufficient control here, which essentially must be counterbalanced by NGOs and the media.

Moreover, in the view of the VÖP expert, the EU net neutrality regulation (European Parliament and Council of European Union, 2015), which is decisive for Austria, restricts itself to the equal treatment of all data only on access networks and does not cover possible discrimination in the transport networks. This would not satisfy the requirements for an up-to-date perception of net neutrality.

2.8 Cyber-attacks

According to one computer scientist, in general, the threat to access to information posed by cyber-attacks in recent years has '*increased dramatically*' in Austria. However, cyber-attacks originating and occurring in Austria are rare; the cyber-attacks that affect Austria overwhelmingly originate from abroad.

In the 'Austrian Strategy for Cyber-security' (cf. CERT 2017), the focus is thus placed primarily on 'critical infrastructures', e.g. energy suppliers, government institutions and hospitals. The VÖP representative does not consider *media and distribution infrastructures of media companies* to be 'critical infrastructures'. The media and communications experts who were surveyed are currently unaware of any significant impairments of public discourse due to cyber-attacks. However, one academic expert assumes that there will continue to be attacks that are not made public. According to experts from nic.at, as yet, politically motivated DDoS attacks have mainly caused image damage.

The C3W expert sees an increased risk of cyber-attacks in the draft bill for a 'security package', primarily due to spyware used by law enforcement agencies, because this software would exploit existing security holes (see also chapter III: 2.5 of this report).

3. Conclusion

Free access to information on the Internet is essentially guaranteed in Austria. The applicable legal standards cover content from traditional media and content on the Internet alike.

If online content is recognised as illegal or unlawful after a judicial weighing of interests, an order to remove the content will be issued to the operator of the website concerned. The specific adjustments to the law, and primarily to criminal law (cyber-bullying, diminishing the wave of incitement) do not represent any trend of criminalising online content. To the contrary, the court verdicts make a preventative contribution to raising awareness in Austria. Practice in Austrian case law shows a good balance between the various fundamental rights.

However, cyber-crime – primarily that originating in Austria – does occur regularly in Austria, but, in the view of the respondents, it has not yet reached an alarming level.

Despite the high level [of freedom] attested, civil-society experts have identified the following weaknesses in freedom of Internet access:

- Prosecution: the system of reporting offices, which has become confusing, lacks efficiency in the area of cooperation of the participating stakeholders and is lacking above all in terms of capacities and expertise (for example, at police departments). The prosecution of unlawful content outside of Austria and the EU is also currently ineffective and is done only with international administrative aid.
- Copyright infringements can cause ISPs to block content on their networks without a judicial decision to this effect and without the possibility of legal opposition (Tschohl, n.y.). Representatives of the Austrian digital economy suggests the establishment of an independent office with judicial competence to avoid having to bear the sole responsibility for this.
- Official secrecy, which seems anachronistic in the age of e-government, generally represents a disproportionate restriction of free access to information – and not only on the Internet. A broad freedom of information law in place of official secrecy would better meet the requirement of Internet freedom.
- Paradoxical practice of removal: because standards relating to the unlawfulness of content in an international environment vary greatly, diverse content falls victim to the practice of removal by domestic ISPs and international providers. From the perspective of users, freedom of access is subject to seemingly arbitrary restrictions.
- Excessive self-regulation: if platform operators act unilaterally and without constitutional proceedings against content that seems to them to be illegal (‘over-blocking’), this violates the principles of transparency, legitimacy, proportionality and responsibility and restricts free speech. Voluntary cooperation in a joint structure with government institutions and civil-society stakeholders could create a remedy.
- Net neutrality: deficiencies in the enforcement of rules for access operators’ data management have come to light in Austria (transport networks and access networks). The observation and discovery of violations against net neutrality have to date been more of a matter for the media and civil-society initiatives than for official vigilance.

II. Freedom of expression on the Internet and regulation of online media

1. Introduction

The Internet has essentially changed the landscape and functions of the media. It has not only become an important means for exercising free expression and freedom of information, but it has also increased the options for communication and information exchange (cf. European Court of Human Rights 2012, 3; Lehofer 2014, 100 et seq.; Heinisch 2014, 6 et seq.). While public life was previously realised predominantly by information distributed by media organisations, blogs, websites and social networking sites (SNS, also called social media) now enable the articulation of opinions and content directly to the public. Due to the increasing use of Internet platforms and services, these now perform the role previously assigned primarily to the journalistic media of creating and providing topics of public communication. Traditional media organisations are losing their unique position as arbiters of the nature and method of the creation, communication and reception of news and of how opinions and ideas are expressed (cf. Schweiger 2017, 11; Coe 2015, 21, 23; Lehofer 2009, 99 et seq.).

The Internet has established itself as an efficient and comprehensive sphere of information, discourse and opinion formation. It offers easy access to enormous stores of information and enables citizens to publicise their own content, to initiate dialogue with political, economic and social stakeholders and institutions and thus to exercise their right to free expression without the scrutiny of traditional media gate-keepers (cf. Schweiger 2017, 2). Moreover, woven deeply into everyday life, blogs, websites and especially SNS are changing the perception of the limitations of communication and information reception (cf. Coe 2015, 21).

As a consequence of the increased use primarily of SNS and their mixture of interpersonal and mass communication, the former borders between the private and public spheres are disintegrating in individual perception. Opinions that were previously held privately or expressed casually and unguardedly only for a selected circle of acquaintances reach the public sphere through SNS, with potentially permanent and wide-reaching consequences. Without the traditional entities of social guidance and scrutiny (e.g. parents, teachers, media), the omnipresent, interactive and predominantly anonymous nature of the online environment results in the spontaneous expression of opinions, while the persons expressing them often have no conception of

responsibility for them and the possible consequences of such expression (cf. Bezemek 2017, 54; Coe 2015, 25, 31; Lehofer 2009, 103).

Meanwhile, deflated practical findings in the literature have displaced the euphoric, technologically optimistic perception of expanding free speech through the Internet. The conquest of the dominant mediation roles has been accompanied by the loss of professional journalistic information processing. The Internet in general and SNS in particular are confronted with large quantities of mass-distributed 'taunts, lies, perceived truths and hate tirades' (Schweiger 2017, 6), and there is a growing suspicion that they are being utilised as instruments of strategic manipulation. This is associated with negative consequences for political knowledgeability, the ability to engage in discourse and opinion formation (cf. Schweiger 2017, 6; Coe 2015, 26), which pose challenges for the complex social balance between fundamental rights and principles (cf. Gagliardone 2015, 7).

1.1 Changes in journalism

While the broad distribution of messages from earlier mass media such as newspapers, television and radio was reserved, today any person can create content and mass-distribute it via the Internet (cf. Gersdorf 2009, 34 et seq.; Fürst, Schönhagen and Bosshart 2015, 328 et seq.; Brown 2013, 4) because the barriers to publishing have largely disappeared (cf. Eldrige II 2017, 51). Alongside online editions of print newspapers and websites for broadcasters, generic online media that did not originate in the printing world (cf. Pfeifer 2009, 47) and blogs that are used to distribute information to the public (cf. Brown 2013, 4) can also be found on the Internet.

These generic online media present a significant challenge for the profession of journalism. If it has already been barely possible to draw a clear line between this and other professions in Austria (such as public relations, corporate communication), then the boundaries are even less clear on the Internet. Self-employed bloggers and so-called YouTubers create content that can be accessed intermittently on a massive scale by fans and followers, making this content similar to editorial content in this respect. At the same time, this content is not subject to the social scrutiny of journalistic editing. Such Internet stakeholders often promote products and brands as 'influencers' and thus transcend the boundaries to advertising and commercial communication.

Much online content is published inside of ‘walled gardens’, primarily on platforms like Facebook, Twitter and YouTube. These private providers generally do not generate their own content, but they offer a space for publication by their users, and often in the context of commercial interests (cf. Imhof 2015, 16 et seqq.). Open access to publication options in walled gardens poses problems when dealing with hate speech and fake news. How much responsibility should, must or may be attributed to platform providers when dealing with content is the subject of public controversies.

1.2 Hate speech

The growing quantity and broad distribution of hate commentary on Internet platforms (cf. Gagliardone 2015, 13) is increasingly viewed publicly and politically as a socially relevant problem and places pressure on free expression on SNS (cf. Coe 2015, 31). However, it is difficult even to make a clear determination of what constitutes ‘hate speech’ (cf. Gagliardone 2015, 7 et seq.; UNESCO 2015, 50).

Stakeholders involved in regulatory proposals draw on various bases for this; prompted by public and political pressure, Internet platforms developed their own definitions of hate commentary that are binding for users and can result in deletion. National governments, on the other hand, invoke cultural conditions; ‘national and regional bodies have sought to promote understandings of the term that are more rooted in local traditions’ (Gagliardone 2015, 7 et seq.). The Council of Europe is attempting to fundamentally outline hate speech in a Recommendation[111] as a ‘general abstract disparagement of entire groups’ (Bezemek 2017, 46). The additional proceedings of the Council of Europe’s convention on cyber-criminality (cf. Council of Europe 2003) and the EU Council’s framework decision (Council of the European Union 2008/913/JHA) require that racist and xenophobic content both online and offline be subject to criminal prosecution (cf. Gagliardone 2015, 26).

However, warnings are being given in the professional discourse on this topic against the implications of criminalising statements of opinion in connection with ‘slander’ and ‘defamation’. The representative for freedom of the media from the OSCE notes a trend in a number of nations of treating ‘slander’ and ‘defamation’ as civil or even

[111] ‘For the purposes of the application of these principles, the term “hate speech” shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.’ (Council of Europe 1997, 107)

criminal issues. Significant restrictions of freedom of the media would be a risk, especially when lawsuits originate from the state, government bodies or public representatives. Disproportionate self-restriction by content producers should be avoided. The OSCE representative therefore speaks out in favour of a fundamental decriminalisation of statements, with the exception of direct calls for violence (cf. Akdeniz 2016, 45).

It is precisely because there is no difference between the penalty for hate speech online and that for hate speech offline that it is recommended in the literature that the special significance of SNS and the Internet not be underestimated. The legislature is prompted to pay special attention to the specifics of hate speech as an online phenomenon when the criminal provisions are updated (cf. Bezemek 2017, 46; Gagliardone 2015, 13). Hate speech on the Internet demonstrates a stubborn persistence in that it remains detectable online in various formats via multiple, in part linked, platforms and over a long period of time. Even after deletion, it can resurface under other names on new platforms or websites. The fact that hate speech is easy to produce and its presence is virtually permanent gives such content online an ongoing relevance for certain population groups. In this way, even ideas and wording into which little thought has been invested and that are not publicly distributed offline obtain access to a wider audience (cf. Gagliardone 2015, 14).

The anonymity of the authors is a hallmark of hate speech. Calls for requiring users to use real names on platforms are met with concerns about limiting privacy and free speech. Anonymity is considered an essential condition for participating in online debates, particularly those that concern controversial topics. Anonymity presents an opportunity for people who are threatened or persecuted to express their opinions without directly putting themselves at risk. In the literature, it is also not considered to be guaranteed that identifiability would lead to less hate speech. The majority of hate comments currently come from pseudonymous sources, which are not considered to be completely anonymous (cf. Gagliardone 2015, 14; UNESCO 2015, 43).

1.3 Fake news and disinformation

It is easier for falsehoods to spread on the Internet due to its anonymity, low costs and the increasing variety of platforms (cf. Unterberger 2017, 41). Fake news is defined as falsehoods that are distributed knowingly; this is a phenomenon that has consistently

been associated with the media. Creators of false reports are often politically motivated and profess to create a ‘counter-public’ to ‘mainstream media’ and to provide the ‘truth’ (cf. Brodnig 2017, 13 et seq.). Fake news therefore spreads faster than factual content (cf. Mihailidis/Viotty 2017, 447), as is shown by statistics on interaction with news content: during the 2016 US presidential campaign, the 20 most popular false reports received more attention in the form of likes, comments and shares on SNS than the 20 most popular reports from traditional media (cf. Berghel 2017, 81; Brodnig 2017, 17). The more often that users react to false reports, the stronger and more problematic the effects of these reports become. False reports were also widely distributed during the 2016 Austrian federal presidential election, including reports of alleged ballot-rigging. A poll taken on behalf of the *Profil* news magazine shows how this unsettled the population. Eighteen per cent of those surveyed did not believe ‘at all’ that the polls proceeded properly and an additional 20 per cent believed it ‘somewhat’ (cf. Brodnig 2017, 21). Fake news has such a strong impact because it confirms assumptions that readers already have. It often escapes their attention that they are dealing with false information. In addition, these reports often circulate in echo chambers where they meet with hardly any criticism. This lends credibility even to absurd content (cf. Brodnig 2017, 107).

This algorithm-based personalisation of access to online content creates an alarming dynamic for the politics of a democracy due to the growing significance of Internet platforms as sources of information. This is particularly the case when users within a platform are not shown any content that contradicts the personal preferences of theirs that have been ascertained and so the access to a variety of information that is essential for opinion formation is limited. This likewise manifests itself in the fact that emotionally charged content is distributed more intensively within this homogeneous environment of perspectives. Knowledge and mastery of these technological options open up new opportunities for stakeholders in strategic communication – e.g. using automation or fake news – to manipulate the process of opinion formation.

This means that fake news can have a warping effect on democracy by influencing how citizens form opinions. The World Economic Forum estimates the distribution of false information to be one of the greatest risks to society (cf. Thiel 2017, 103).

2. The results of the expert survey

2.1 Freedom of the media

In the estimation of the respondents from the ORF, the VÖP and one online medium, Austrian legislation does not restrict the exercise of freedom of the media on the Internet. In consensus with the report on worldwide freedom of the press by Reporters without Borders (in which Austria took 11th place), the experts surveyed do not designate any Internet-specific restrictions of freedom of the journalistic media in Austria, with two exceptions:

For one, the respondents from the ORF criticise Internet-specific obstructions to free speech in the ORF-G, such as the restriction of the quantitative output of online articles, the graduated bans on forum posts and the seven-day rule, according to which content may remain retrievable for only one week after it is distributed on the Internet. The fact that these restrictions are thus not justified is also confirmed by respondents who do not belong to the ORF.

For another, in its *Weißbuch für den Medienmarkt Österreichs* [Whitebook for the Austrian Media Market], the VÖP criticises the fact that the Audio-visual Media Services Directive (AVMSD) does not cover online platforms from third parties, even if they are active on the Austrian market and therefore come into direct competition with domestic services, which are subject to the Directive (cf. VÖP 2017, 32). The ban on representations of hate/violence and the requirements to protect consumers, children and youth are stipulated specifically at the content level (ibid).

Moreover, free speech on the Internet is also affected by general restrictions. This is why the representative of the VÖZ expressed concerns with respect to the General Data Protection Regulation. He especially criticises the unclear distinction regarding which law (media law or the data protection law) applies to the publication of personal data. A possible penalty of 20 million euro for the unlawful publication of personal data has the effect of a muzzle, which would influence reporting.

2.2 Journalism

The same rights and duties apply to journalists online as do offline, and the expert from C3W does not see any preference or disadvantage with regard to this. In the opinion of

experts from the ORF and academia, the legal protection of journalists on the Internet, is also like that off the Internet.

The VÖP representative sees a reversal of circumstances, particularly with respect to the threshold of free speech and protection of privacy:

'While, as a rule, journalists in the traditional media sector are the same who make use of the rights to free speech and freedom of communication and who must respect the privacy of third parties in their conduct as journalists, social media, etc., reverse the distribution of roles. Now users of social media make use of their right to free expression and harshly criticise journalists (as well), and, in doing so, occasionally violate the fundamental boundaries of the affected journalists' private spheres.'

The representative from the Democracy Centre Vienna and a respondent from the Digital Society argue for the sensitisation and adequate training of the police for cases where boundaries are crossed, which journalists and Internet users are particularly affected by on social media, for example, through hate speech, hostility and threats. Aside from that, in their opinion, authors of hate speech should be more consistently identifiable and government cooperation with intermediaries (e.g. Facebook) should be improved in order to combat hate on the Internet more effectively. Journalistic practice does not directly restrict hostility on the Internet, even when the rapid, immediate and far-reaching distribution of such hostility could be painful for individual journalists.

Big data analyses also represent an additional challenge for journalistic practice (on this, see also chapter III.2.3 of this report). One media expert fears that comprehensively linked stores of collected data that are compiled without the approval and knowledge of data subjects could make it more difficult for journalists to access information (e.g. due to revocation of a licence).

2.3 Hate speech and fake news

The experts of the VÖP and the ORF note an influence on and disruption of Internet discussion in Austria by 'trolls' and fake news. Both are pervasive and can be found on all (unmoderated) fora for Austrian newspapers, says an academic expert. False reports spread in Austria predominantly via SNS, an expert from the Democracy Centre Vienna explains. One academic expert also cites the establishment of portals such as *unzensuriert.at* and *politiknews.at* on which fake news is distributed. Recent years have seen intensified instances of false reports in pre-election periods and on politically

polarising topics. The respondents from nic.at and ISPA note a peak in connection with the increased migration movements in 2015/2016. Since partisan media and politicians participate significantly in their distribution, in the opinion of the expert from Civil Courage and Anti-racism Work (ZARA), this is associated with strategic exploitation for political purposes.

The impact of actors who are organised and paid to influence free speech has previously been described as hardly worth mentioning. Currently, according to experts from ISPA, it is mainly individual persons against whom criminal proceedings could be initiated. The extent to which social bots are used in Austria in order mainly to influence opinion formation on SNS is characterised by experts from the VÖP and C3W as little known and researched.

The new and diverse options for expression on the Internet fundamentally intensify the problems of fake news in the estimation of one academic expert. For the representative from the VÖP, these problems are amongst 'the most important issues for the future of online media' in Austria.

The growing distribution of false reports is increasing the importance of new phenomena like fact-checking websites (mimikama, kobuk, Addendum [the Quo Vadis Veritas Portal of Dietrich Mateschitz]) for Austria. A representative of the Digital Society notes in addition to this that opposition to fake news generally garners far less attention than the original (false) report. Therefore, efforts to identify the creators of fake news must also be increased.

However, the distribution of fake news is also viewed as an enhancement and chance for serious media and qualitative journalism to regain 'lost trust', as noted by representatives of ISPA and the ORF. In connection with this, the representative of the VÖZ indicates that traditional media and their electronic offshoots must work with greater focus with respect to source checking and transparency so that the core product of the media represents a gain for users.

However, imparting the corresponding media competence is also among the key measures here, according to the representatives from ISPA and the Digital Society. Representatives of the ITA therefore consider mainly the acquisition of digital competence to be of central importance because censorship measures represent an even greater threat than the fake news itself.

3. Conclusion

Internet freedom is guaranteed on principle for online media and journalists in Austria.

The Internet has starkly changed the journalistic profession, on the one hand due to the introduction of new journalistic and pseudo-journalistic stakeholders (bloggers, YouTubers, influencers), and on the other due to the numerous feedback channels with which users can comment on journalistic articles. (Anonymous) threats and hostility have increased in this way, which could negatively impact journalistic behaviour.

The experts surveyed interpret hate speech as a negative side effect of free speech, but they do not see any specific need for action with regard to additional protection for journalists. This is sufficiently guaranteed by criminal law and the protection of the private sphere.

The limits set in the ORF-G for the availability of online content represent a special case. The seven-day rule and the limitation of the quantity of online postings limits freedom of expression and likewise the freedom of citizens who have paid for the services of the ORF with their licence fees to receive messages.

In total, the mass media, which are oriented towards the skilled and continued monitoring of societal opportunities and risks, have experienced a decline due to the Internet. The attractiveness of communication intermediaries on the Internet (Facebook, Google, Instagram, Twitter, YouTube, WhatsApp, etc.) for the advertising sector is eliminating the economic foundation of the primarily advertising-financed traditional mass media bit by bit, The continued monitoring of developments on the Internet that is important for guaranteeing Internet freedom thus represents a challenge for civil society that the traditional mass media are hardly able to negotiate single-handedly anymore.

III. Data protection and the protection of the private sphere

1. Introduction

If the concept of protection of privacy also covers physical and spatial aspects, then, in connection with the Internet, this is relevant above all to the protection of and control over personal data (data or information privacy) and communication (privacy of communication) (cf. Cannataci et al. 2016, 11; Mendel et al. 2012, 11).

The protection of privacy has a complex relationship to freedom of expression, the right of access to information and to security issues, in particular. The business practices that have become common on the Internet exert pressure on the private sphere and its protection. The pervasiveness of the digital world in everyday life generates more and new personal data that it is becoming ever easier and more cost effective to collect and process as a basis for the business models of Internet intermediaries using a growing number of new data technologies (cf. Cannataci et.al. 2016, 9; Korff/ Brown 2013, 3; Mendel et al. 2012, 13 et seq.).

Mobile Internet use via smartphones creates a specific dimension of risk, as it allows not only the precise localisation of the device but also the convergence of various sensors, chips, platforms and applications that each access certain information. The combination of these creates a far more comprehensive data source than the individual data alone. These convergent data sets, which are fragmented and yet at the same time hardly able to be overseen in everyday use, elude individual data control (Mendel et al. 2012, 35; Korff and Brown 2013, 3).

The challenges of protecting privacy thus arise not only alongside specific technologies, but are created from their combination with an environment of ongoing data collection and processing in which individuals hardly have any more influence on the use of personal information. The relevance becomes apparent in the potential convergence of the Internet of Humans with an Internet of Things and with nanotechnology (cf. Cannataci et al. 2016, 92; Korff and Brown 2013, 4 et seq.).

New processing capacities enable the efficient storage, processing and analysis of enormous quantities of data as ‘big data’. This involves merging direct usage data with additional, in part public, data sets. From the perspective of data protection, it is above all the reuse of data for purposes for which no consent has been given, as well as the removal of any anonymity with ‘data profiling’ or ‘data mining’ applications, that are generating anxiety (cf. Cannataci et al. 2016, 95; Mendel et al. 2012, 15 et seqq.; Korff and Brown 2013, 5 et seqq.).

There are similar concerns over the protection of privacy associated with the increasing prevalence of cloud applications when the distribution and security of personal information by cloud providers remain unclear or data is physically stored in countries

with inadequate data protection laws (cf. Cannataci et al. 2016, 93 et seq.; Korff and Brown 2013, 8).

1.1 The state

In the Internet the state has a tool that enables it to provide and expand cost-efficient and personalised services and information to citizens (e-government). These are based on large quantities of personal data from the entire population. This means that e-government can only work through the collection, storage and scrutiny of sensitive data by the state. Data-protection concerns arise when the data is not collected transparently or protected adequately from cyber-attacks or is stored by third parties. The change to a model of governance that relies on data processing is criticised in the academic literature when, in this context, automated decisions are taken using back-office data processing and analyses without the consent and knowledge of the data subjects. Without suitable legal mechanisms, data subjects are put into a vulnerable position (cf. Cannataci et al. 2016, 18; Korff and Brown 2013, 13; Mendel et al. 2012, 17, 19).

Technological progress continues to widen the gap between the applicable laws, the actual threats to privacy and data protection. Open questions of the ownership, rights and control over continuously collected data make effective protection of individual privacy more difficult. These problems come to a head particularly in the regulation of big data and data profiling (cf. Cannataci et al. 2016, 29 et seq., 97 et seq.; Svenson et al. 2016, 34). If this also concerns companies, disclosures in this context by government stakeholders suggest more and more the magnitude of mass surveillance using new technologies (cf. Cannataci et al. 2016, 16 et seq.; Mendel et al. 2012, 17).

1.2 Companies

Internet business models that rely on the collection and commercial exploitation of data for marketing purposes are one focus of discussions on the problems of privacy and data protection. High demand is driving the development of new technologies for more efficient and more comprehensive collection, storage and processing of ever greater quantities of data. Big data and data profiling allow increasingly precise insights into target groups and persons and, in the process, make the dissolution of the private sphere into a core business. Companies keep secret which data are collected and analysed and how this is done as the foundation of their business activities. Data-protection concerns exist vis-à-vis trading in data, questions surrounding the security of

the databases and the increasingly automated processes between data collection and exploitation (cf. Cannataci et al. 2016, 16; Mendel et al. 2012, 17, 19, 22).

Intermediaries and ISPs play a significant role in the Internet economy. Because their services enable individual Internet access and the transmission or processing of information, they also obtain access to and control over personal usage data (cf. Mendel et al. 2012, 19). In view of their central position, concerns are increasingly being voiced regarding whether existing regulations sufficiently guarantee the protection of privacy. This is associated with the question of whether intermediaries (e.g. Facebook, Google, WhatsApp, YouTube) are to be classified as media companies and whether the applicable rights and duties also cover these companies.

There is scepticism in the literature vis-à-vis pure self-regulation with respect to data protection. Too often does the need for regulation and business interests clash with one another. The current practice of obtaining consent to complex terms of service as a tool of data protection regulation is criticised in particular. The user consents to the general terms and conditions in order to be able to use the services, often without having read or understood them (even if the user confirms having done so by ticking a box that s/he is compelled to tick). Data-protection conditions contained in these terms are not required to correspond to national provisions (cf. Cannataci et al. 2016, 26-29). Conversely, it is necessary to protect Internet traffic from potent attacks by interest groups or government stakeholders. This is a problem that becomes acute when intermediaries and ISPs are in involved in government surveillance (cf. Cannataci et al. 2016, 17; Mendel et al. 2012, 20).

Growing data-protection concerns are also arising vis-à-vis providers of social networks, search machines and cloud services. The character of social networks lures users into treating personal data lightly with little awareness of the risks or how to use data protection settings. The use of cloud services (primarily with respect to international providers) can result in a loss of control and a lack of legal security if no legal claim can be derived from the [provider's] terms of service (cf. Mendel et al. 2012, 20 et seq.).

1.3 The individual

With the integration of the potential of new technologies into individuals' everyday lives, online activities intentionally and unintentionally generate data that can become

the starting point for a threat to the private sphere. Therefore, questions regarding awareness and competence of individuals when dealing with personal data are central (cf. Cannataci et al. 2016, 14; Mendel et al. 2012, 22 et seq.). If there is a general gap between the high abstract value of the private sphere and actual online behaviour, then it turns out that the awareness of the problem depends upon sociodemographic factors, especially education. Children and youth are described as particularly threatened groups (cf. Svenson et al. 2016, 39, 50 et seq.; Mendel et al. 2012, 11). The difficulties of raising awareness lie in the fact that the consequences of hardly perceptible attacks on privacy emerge only after long delays and that the cause of discrimination in the affected individual's everyday life can hardly be traced back to data protection violations from years ago (cf. Čas et al. 2017, 7).

At the same time, there is the question of whether the speed, range and complexity of the diffusion of information in a society that is comprehensively pervaded by technology do not exceed individual skills and abilities and stand as obstacles to decision-making processes and scrutiny. This problem becomes apparent in the practice of obtaining consent to non-transparent terms of service. The exchange of personal data for (free) services that is at the core of many online business models is overwhelmingly to the detriment of users because they are scarcely able to control their own information online (cf. Cannataci et al. 2016, 14 et seq.).

Add to this that the anonymous use of services and applications is circumvented by new technologies that remove and bypass the private sphere with the analysis of large quantities of data. However, anonymous use represents an important element in the balance between data exploitation and privacy protection (cf. Korff and Brown 2013, 17 et seq.).

2. The results of the expert survey

Everyday life for Austrians is increasingly pervaded by the use of interlinked digital devices and applications that create an environment of ongoing collection, storage and exploitation of personal data, which increasingly invades the private sphere. This was particularly apparent to the surveyed experts through the widely distributed use of smartphones in Austria. Cloud applications also give cause for essential concerns about effective data protection.

It is becoming more difficult to firmly specify the threat to privacy and free speech in Austria arising from big data analyses. Because of the inherent potential for control, filtering data packets with ‘deep packet inspections’ is considered a severe restriction of Internet freedom. At the same time, access providers can use it as a tool for regulating data streams. The experts assign particular relevance to plans to introduce government surveillance software because of their topicality. The increasing threat of unlawful access to collected data poses questions of data protection, particularly due to cyber-attacks in Austria’s companies and public institutions.

Individual awareness of personal data protection is of central importance to the experts. However, the protection of privacy is also the task of an effective legal framework that focusses on improvements (and criticism) of the General Data Protection Regulation and the Data Protection Amendment Act.

The problems and challenges indicated here will be discussed below from the perspective of the surveyed experts on civil society.

2.1 Smartphones

Austria is characterised by comparably low costs for mobile Internet in connection with greater distribution and intensive use of smartphones. In this context, experts from academia and civil society (C3W, ÖIAT, the University of Salzburg) characterise the accompanying consolidation of personal data via various sensors, platforms and applications and the fragmentation of individual control over these data as urgent and ‘extremely underestimated’ problems for Austria.

On the one hand, this concerns the general regulatory conditions in Austria, which must be adjusted to fit both the technical options for data collection and processing and the business models for data exploitation. The adoption of the General Data Protection Regulation (GDPR) in 2018 would mean an update to the Austrian Data Protection Act of 2000. However, this Regulation also guarantees only insufficient protection of personal data on smartphones in many areas.

On the other hand, the awareness of problems surrounding the sensitivity of personal data amongst users in Austria is determined to be weak. According to one media expert, users show little care when configuring the settings for their data protection options in hardware and software. However, users could scarcely gauge the technological complexity of smartphones, and consenting to general terms and

conditions can no longer be considered an act of autonomous control over personal data. The expert from the ÖIAT described the passivity, resignation and fears for the future mainly amongst youth over the later impact of collected and analysed personal data as a consequence of lacking options for individual control.

Experts from the C3W and the Association for Anti-piracy in the Film and Video Industry (VAP) agree: suitable media competence is lacking in Austria. The topics of 'money for data' (C3W) and the clarification of 'tracking and profiling' (VAP) have been openly addressed with too little frequency. Training for appropriate media competence is understood to be primarily a government task due to the growing economic interest in data.

The experts from Austrian companies also give a bad report with respect to awareness for the consequences of data collection through smartphone use because company standards on the use of SNS applications on company smartphones are largely lacking, and both private and company data are barely protected.

2.2 Cloud applications

The increasing use of cloud applications indicates the trans-national dimension of the Internet because data is exploited globally and effective data protection is difficult to implement. This creates data-protection problems when personal data are stored to cloud applications that have company headquarters located in countries in which the legal provisions exhibit a lower level of data protection than Austrian, respectively EU, standards. However, data protection experts and computer scientists describe the marketplace principle of the GDPR as an improvement. Conversely, there are questions about enforcement and how effectively this law can be enforced outside of Austria and the EU. This is especially the case when there is no sound and effective legal basis for international data streams, says the data protection expert from the Chamber of Labour.

Targeted sample enquiries of the employees of the C3W reveal that, in the practice of global data networking itself, concerned companies seem to no longer have any clear notion of the physical location of the data that they process. However, when it is no longer transparent which law applies, the right to data protection becomes fiction.

In Austria, fundamental reservations are being expressed regarding the lack of control over one's own data vis-à-vis cloud services; these are manifested in questions such as:

What happens to deleted data? What happens if the service closes down? Who has what right of access?

The experts from the C3W and nic.at note little awareness in Austria regarding the scope of the data protection issues that are associated with the use of cloud applications. They add once again that, due to the complexity of the material, consenting to general terms and conditions can no longer be considered an act of autonomous control over personal data. According to the consumer protection expert, since the average consumer knows little about the storage practices of cloud services and, in contrast to the situation with providers, little transparency is created, no specific cases of data protection problems can currently be specified in Austria.

An expert from the VAP criticises the extensive exemption that cloud services have from liability vis-à-vis the content that they process through their services. Cloud providers thus have no incentive to let 'commercial duties of care and inspection' prevail. Drawbacks would arise primarily for rights-holders – e.g. in the creative industry – if cloud providers distribute copyright-infringing content.
In particular, there are reservations vis-à-vis anonymity for cloud services.

2.3 Algorithm-supported big-data analyses

There are also problems in Austria associated on principle with the fully automated collection, processing and exploitation of large quantities of data using confidential algorithms as the centre of the big data paradigm. This is because, as much as data is considered the economic basis for a growing industry, very little is known about the distribution and application of big data analyses in Austria. Technology corporations with business models that constitute the commercial exploitation of large quantities of data are considered to be forerunners. Moreover, it is assumed that companies offer the development and analysis of data for the purposes of risk analysis and marketing as a commercial service. The study by the ITA on behalf of the Vienna Chamber of Labour entitled 'Credit Scoring in Austria' offers only limited insight, but it shows the potential scope of problems with big data in Austria. Data is summarised into specific profiles (in this case, for financial solvency) without the knowledge of data subjects and this influences significant areas of everyday life without the data subjects knowledge. Since the underlying calculation model is considered to be a trade secret, there is no insight into which data form the basis for decisions.

With reference to the ‘Credit Scoring’ example, commercial big data analyses in Austria are described as a barely regulated and largely non-transparent sector of business. In view of the consequences, based on this reference there exists in the literature a call for action for an Austrian ‘anti-scoring law’. However, the data protection experts surveyed currently rule out ‘predictive policing’ for government applications of big data in Austria.

The experts from academia and civil society are unanimous in their basic assessment: algorithm-driven data collection and analysis taken as a basis for commercial and political, respectively government, decisions signifies a broad loss of transparency. Technologically implemented calculation models do not in any way ensure an objective approach, but rather their emergence, data base and weighting should be viewed as expressions of social relationships and interests. This is associated with a risk of discrimination and manipulation.

The academic experts emphatically call for broad social discourse on the risks arising from big-data applications and their underlying algorithms. Appropriate transparency rules and public regulation institutions (e.g. algorithm ethics commission, algorithm technical inspection association, codes of conduct) stand at the centre of this discourse.

Austria’s existing legal regulations, as well as the GDPR, would only insufficiently cover these new challenges for the protection of the private sphere. Indeed, one computer scientist indicates that the GDPR contains significant principles in the requirement of ‘lawfulness, processing in good faith and transparency’ when personal data is processed, but these would not encompass the complexity of modern algorithms and therefore would not be adequate to meet the challenges. According to the expert from the VAP, the GDPR is lacking, among other things, standards for scientificity, certificate regulations, effective scrutiny and oversight, comprehensive bans on discrimination, and understanding that conclusions are based on correlation rather than causation and that trade and business secrets contradict requirements for transparency.
The expert from the C3W emphasises the need to supplement structural measures with data protection and media-competence measures from a long-term perspective and thus strengthen individual data control.

2.4 Deep packet inspection

The technical investigation of the content of data packets using deep packet inspection (DPI) is unlawful in Austria due to the lack of consent from data subjects to the analysis of their personal data. However, the data protection experts from the ITA refer to an important distinction: does the DPI take place in Austria and/or are Austrian data affected?

Regarding Austria, the experts from civil society and the technology and media sectors are in agreement that there are no known cases of data protection violations and attacks on the private sphere using DPI. However, experts voice conjectures about the utilisation of data management measures in networks by access operators, which utilisation raises questions about the proportionality of prioritisation. Several experts from academia, civil society and the technology sector suspect that medium and large firms, public institutions and authorities also resort to DPI for the purpose of 'misinterpreted self-preservation'.

According to the data protection experts from the ITA, there is also a fear that, upon exposure to the machinations of intelligence agencies, Austrian data streams will also be subject to surveillance using DPI. However, according to one computer science expert, evidence of actual violations of privacy and data protection resulting from the use of deep packet inspection is very difficult to produce.

2.5 Trojan horses

The use of surveillance software (Trojan horses) by law enforcement agencies is not permitted in Austria. The Austrian Ministry of the Interior affirmed in a parliamentary enquiry on this topic that no Trojan horses would be used.

Although the use of these is considered under the law to be seriously questionable, the experts from ISPA refer to draft proposals of the past, the adoption of which could only be prevented with broad public criticism.

Multiple experts are likewise critical of plans for a 'security package' that would, among other things, enable the use of software to monitor encrypted communications technologies. Along with questions of cyber-security, there are predominantly concerns regarding broadly designed surveillance of communication. Experts on the digital economy say that potential encroachments on the private spheres and free speech of

journalists could result in a chilling effect on the performance of investigative media work.

2.6 Data protection in companies

Multiple academic and civil-society experts ascribe low data protection awareness and partially lacking knowledge of up-to-date data protection to Austrian digital economy companies.

There is a gap between the existing legal framework of the Data Protection Act of 2000 and practical enforcement. If data protection measures have also been provided for under the law before, low fines for data protection violations have been the main reason that enforcement of the law with regard to companies has been viewed as inadequate. In this respect, experts (epicenter.works, ITA, nic.at, ÖIAT) expect a gradual improvement of the data protection situation in Austria's digital economy companies once the GDPR takes effect.

Different experts assess the scope of the improvements differently. Despite the severe fines with which lacking data protection could be punished starting in 2018, the expert from the C3W sees only little progress thus far. The future mandatory appointment of a data protection officer will be a drawn-out process in companies, which would evidently rather budget funds for possible fines. Data protection would adversely affect the business interests of many companies, since by now a significant share of their turnover originates from the sale of data generated in their own systems.

The data protection experts of the ITA note an 'enormous' boost in awareness at the company level with the GDPR – this is due both to more intense penalties and to better regulations for handling personal data, as well as new principles like the data protection impact analysis. Enforcement is still open, but the GDPR has made data protection into an area of development for companies in Austria.

In addition, the expert from the VAP calls initiatives for self-regulation important complementary measures to government regulation for achieving security on the Internet with the involvement of all affected stakeholders.

2.7 Cyber-attacks on companies

The protection of data from Austrian digital economy companies from cyber-attacks must be assessed in terms of varying company sizes. The computer scientist from the

University of Salzburg concedes that larger companies need more, but not necessarily better, protection from cyber-attacks. According to the experts from nic.at, small and medium-sized companies without core IT competence are quickly overwhelmed by up-to-date protection measures. The expert from the C3W says that lacking knowledge, including regarding consequences, and limited financial means are the main reasons why Austrian companies have viewed data protection as only a side issue until now.

At the same time, the experts describe a drastic change to the threat situation from cyber-attacks (DDoS, CEO fraud, spear phishing and ransomware), through which the effectiveness of traditional protection mechanisms (automatic updates, firewalls) are eroding and the involvement of employees as a significant protection measure is gaining in importance. The companies are also ascribed a poorly developed awareness in this regard, e.g. with respect to the use and linking of private devices with the company network, says the expert from the VAP.

In spite of this threat situation, experts on the digital economy emphasise the high data security standards of Austrian companies. The Computer Emergency Response Team (cert.at) is considered an important institution. It quickly sends out warnings about IT security problems. Austrian network operators must report significant security incidents vis-à-vis RTR GmbH – and vis-à-vis the data subjects and the data protection authorities in the event of data protection violations. In addition, a ‘well-functioning self-regulation’ is established in the digital economy with respect to security issues. However, an academic data protection expert from the ITA describes the resources of Austrian CERT as insufficient in the face ever more elaborate cyber-attacks.

2.8 Public data at private companies

The storage and processing of data from public institutions is also outsourced to private companies in Austria. Multiple academic and civil-society experts (communication studies, computer science, C3W, epicenter.works) view this trend with ‘great scepticism’ and as a ‘major problem’ with respect to data protection. Control over broader exploitation of data, merging databases and corresponding legal enforcement are only conditionally possible.

The data protection experts of the ITA concede that Austrian officials and public servants basically have a high level of data protection awareness. At the same time, there is a perceived pressure on public institutions to pursue efficient, up-to-date new

paths to providing public services. Awareness and knowledge of good data protection solutions must be found in the public sector if IT and data represent a core professional competency. Data protection is quickly lost sight of in other industries with the use of predominantly free services.

Most examples come from the areas of academia and education, where student email accounts are run via Gmail (Google), which allows academic achievement (e.g. through automated grade notifications) and health information (when students excuse themselves from instruction due to illness) to be viewed. There are also data protection concerns associated with the conversion of university libraries to the 'Alma' system because all inventory and user data are stored in the manufacturer's cloud.

In this context, the expert from the C3W views with a critical eye the strategy of large US software concerns of pushing their customers, public institutions amongst them, into [using] cloud applications. An expert from the ÖIAT cites the use of the Microsoft cloud throughout the education sector for entire school classes using pupils' real names as an example. In addition, one media expert cites a case where unsecured confidential data of 400,000 Austrian schoolchildren was stored on an unsecured server in Romania.

The data protection experts from the ITA say that public institutions in particular serve as forerunners for data protection in Austria and should place a special focus on compliance with the European legal framework when rendering their services.

2.9 Cyber-attacks on public data

Public institutions also serve as models in the area of cyber-security. According to the data protection experts of the ITA, the security level must be distinguished between various competence areas and the size of the organisation: the less that data protection and IT are considered the core competencies and the larger the institution (e.g. the more interfaces), then the larger the potential data protection risks are. Or: the more critical the role of the public, respectively government-related, data, the higher the quality of protection from cyber-attacks is assessed. The surveyed experts from national defence and the Federal Data Centre attest to high security standards and continuous efforts at improvement. However, comprehensive protection of data cannot be assumed even in this case, says the expert from ZARA and one computer scientist. An expert from the University of Salzburg also notes that 'today, even the biggest

ISPs' are 'overwhelmed by DDoS attacks with botnets from IoT devices' and that 'too little value is placed on backup (network) structures'.

Less central or governmentally relevant public data could also be of interest for data abuse in connection with big-data applications. According to the data protection experts of the ITA, this could result in a general threat to public institutions. Apart from technological security measures, the expert from the C3W refers critically to lacking security awareness amongst employees in politics and administration. The communication studies experts also assume a general accumulated need with respect to the protection of public, respectively government-related, data from cyber-attacks.

2.10 Data-protection awareness

Multiple experts ascribe only moderate or completely lacking awareness amongst Austrians when handling their data in everyday online business. Carelessness, complacency and lacking sensitivity vis-à-vis the transmission of personal data characterised their dealings with primarily private commercial providers and their mostly free services. Even where there is fundamental knowledge of data-driven business models, this hardly comes into everyday use ('the privacy paradox').

The experts from nic.at discern greater awareness with respect to personal data protection amongst Austrians when it is a matter of the consequences of monitoring and surveillance, primarily when this results from government measures. According to the representative from the VAP, Eurobarometer 443 on e-privacy (European Union 2016) showed that protection of privacy in communication in Austria is below the European average, but above-average measures are often taken to prevent online monitoring.

The experts from the C3W, ISPA and ZARA cite the costs in terms of time and money, the low availability of alternatives to the free services and devices from companies with data-driven business models, as well as competence for self-determined individual data control that is characterised as low, as obstacles to self-determined handling of personal data in everyday online use.

The data protection expert from the Chamber of Labour welcomes the embedding of measures for increasing media competence and raising awareness into the regular school system as a subject of instruction (this is currently being tested in the 'digitale Grundbildung' [basic digital education] pilot project). This long represented a lack, and

attempts have been made to offset it with additional events. The ‘Safer Internet’ initiative has been cited as an example of good practice in youth work. The knowledge-gap effect that manifests itself amongst difficult-to-reach groups is cited for the area of adult education.

It is an essential task of the state to address this. Moreover, raising awareness is a task for all of the stakeholders involved. More effective approaches must be more easily organised and interlinked.

Conversely, competent handling of personal data on the supply side would be made more difficult or even impossible with difficult-to-understand data protection guidelines and settings.

Therefore, along with imparting important media competence, multiple experts call for the improvement of structural data protection measures. The responsibility for data protection should not rest exclusively with users, but rather it should be a part of the development and provision of devices and services (privacy by design) and of corresponding duties of Internet and platform providers (VAP expert).

2.11 Data protection legal framework and the General Data Protection Regulation

For the data protection experts of the ITA, the legal principles and tradition of protecting personal data in Austria are a good testimony, as is the Data Protection Act of 2000. However, criticism is levelled at legal enforcement, which in practice has resulted in largely ineffective statutory data protection in Austria thus far. The data protection authorities are under observation in this respect. One data protection expert on consumer protection indicates the two-pronged nature of the courts of first instance and the data protection authorities. Those seeking legal protection must sue private legal persons. Due to the cost risk of proceedings, concerned parties must refrain from lodging complaints or initiating lawsuits. Minor administrative penalties would also result in little preventative effect for potential data protection violations. The expert from the Chamber of Labour and the expert from epicenter.works agree with an oft-voiced and long-standing criticism that the data protection authorities suffer from a lack of competence and resources that does not correspond to the scope of their tasks. To summarize, the experts have determined that the legal framework for data protection is not up to date and needs to be caught up.

In contrast, the GDPR and the Austrian Data Protection Amendment Act would send out positive signals. However, the decisive, but still unanswered, question remains that of more effective enforcement, say the experts from the ITA. While data protection awareness is discernibly increasing at present, it is still doubtful whether the threat of penalties is sufficient for the long term. Regulations that better enable data subjects to enforce personal data protection even in court are as necessary as more resources for prosecution.

However, the potential of the GDPR and the Austrian Data Protection Amendment Act is also a source of basic concerns. For this reason, experts from civil society (epicenter.works) warn of serious deficiencies in the development (assessment period is not observed) and the content of the Data Protection Amendment Act. The academic experts of the ITA particularly criticise the stipulated immunity of the authorities with respect to data protection offences and emphasise the forerunner function that the public sector must perform in matters of data protection.

There is even some criticism of the GDPR in Austria. The data protection expert from the Chamber of Labour draws attention to the basic enforcement problems in the implementation of the ‘right to be forgotten’. She criticises the fact that enforcement is left to companies, which is tantamount to outsourcing constitutional responsibility. The standard must remain a lower threshold to access to a legal ruling, whereby arbitration boards represent a conceivable approach to a solution. Without such support, it is feared that data exploitation interests will take priority if data subjects must prove their interest in confidentiality vis-à-vis the ‘overriding justified interest’ of the company in collecting data. In this context, the experts of the ITA also refer to the problem of large quantities of ‘automated individual decisions’.

In the view of the expert from the Chamber of Labour, fundamental questions of data protection also would not be clarified with the GDPR. Thus, it would seem that data protection law has also not been thoroughly considered at the European level, but rather it is made up of various laws with little harmony between them and that partially contradict each other. This becomes apparent, for example, in contradictions between the planned ‘e-privacy’ regulation and the existing GDPR (cookie paragraph, offline tracking).

Certain problems would certainly also remain with the new data protection regulations. The legal experts of the BMJ therefore stress the importance of broad civil-society

initiatives, which continuously illustrated problems and clarified grey areas with self-initiatives. According to the representatives of ISPA, Austria exhibits an active civil society in the area of data protection in comparison with other countries.

3. Conclusion

The assessment of data protection and the protection of privacy in the digital age comes off as mixed in Austria. One the one hand, personal data protection seems to be threatened by the potential of technical developments. Personal data are collected, stored, processed and supplied for commercial exploitation on a grand scale with or without the consent of data subjects.

On the other hand, the survey in Austria gave few specific clues to concretise these threats. Outside of experts and groups of experts, the threat to privacy posed by networked information and communications technologies is a side issue for the public. Data protection law scarcely registers; lawsuits are rare and there are low penalties in the event of judgment against the defendant.

The following key points can be taken from an investigation of the situation in Austria:

- Data protection as a ‘black box’: embedded in global business models, leaks out only to small extent via practice of commercial exploitation of the personal data of Austrians. Studies by Christl (2014) and the ITA on selected aspects (Rothmann et al. 2012, 2013, Krieger-Lamina 2016) give insight and reveal the urgency with which data protection has developed in Austria, including with regard to issues of Internet freedom.
- There is little awareness of the problems of smartphone data tracks: with public smartphone usage at 81.3% (cf. Gadringer et al. 2017, 58) and correspondingly higher rates amongst youth, attacks on privacy that originate from these devices are considered to be an obvious and therefore urgent problem for Austria. ‘Smartphones and the apps installed on them are a biggest “gateways” for companies that collect personal data on users’ (Christl 2014, 32). The combination of a multitude of sensors (microphone; camera; GPS receiver; movement, location, light, proximity and magnetic field sensors) creates a broad data track. Software (apps) accesses sensors and data via a system of permissions, links them to personal user profiles and enables deep insight into the personalities and everyday lives of Austrians (cf. Christl 2014, Rothmann et

al. 2012). There is little awareness of this problem amongst the population. Along with the long-term perspective of data protection and media competence, additional structural legal measures that continue to ensure the protection of privacy in Austria are also needed.

- Uncritical use of cloud services: there are fundamental concerns vis-à-vis cloud services with respect to legal certainty and authority over the control of individual data. Data protection awareness and a corresponding legal framework should prevent attacks on privacy.
- Little knowledge of big data analyses: data is handled and bundled into personal profiles without the knowledge of data subjects, including in Austria. Commercial big-data applications can be considered to be assessments of individual solvency and are just the tip of the iceberg (on credit scoring, cf. Rothmann et al. 2013). Broad social discourse on the risks of discrimination and manipulation using big data and a political decision-making process regarding transparency rules, and not just at public institutions, are still yet to come in Austria.
- Hope for the GDPR: many of the aspects mentioned are seized upon with the GDPR and the Austrian Data Protection Amendment Act. A Europe-wide harmonisation of the data protection law, the ‘right to be forgotten’, the marketplace principle, strengthening the data protection authorities, intensifying financial penalties, and data protection officers for companies, as well as essential, forward-looking principles such as ‘privacy by design’ and ‘privacy by default’, will contribute to an improvement of protection of privacy in Austria.
- Legal enforcement is the key issue: while there is a discernible growth of data protection awareness amongst companies at present, it is doubtful whether the threat of penalties is enough in the long term. Prosecution, primarily by the data protection authorities, requires more resources. However, regulations that better enable data subjects to enforce personal data protection in court are also necessary.
- Digital media competence: Austrians exhibit hardly any problem awareness when handling their data in everyday online business. Making media

competence a subject of regular instruction in the school system would signify an improvement.

IV. Actual accessibility

1. Introduction

The global changes in technology have brought about a growth in economic productivity, global collaboration and electronic commerce and a change both in governmental issues and in society (cf. Pick/Sarkar 2015, 1 et seq.). The latter has quickly changed into an information and network society due to the new information and communications technologies (cf. Castells 2000, Meikle and Young 2012, Van Dijk 2012; Wessels 2013, 17). This generally signifies simplified access to and exchange of information for the members of this society (cf. Ragnedda 2017, 9). Rather than achieving an equalisation between high- and low-status members with respect to the state of their knowledge and information, in practice the digital change has resulted in an intensification of existing inequalities. New inequalities are created (cf. Wessels 2013, 17) and the gap between the group with greater access to communication distributed via the media and that with lower access is growing (cf. Zillien and Haufs-Brusberg 2014, 9).

Next to the requirements for access, actual use is central. Using the Internet is often more challenging cognitively, technically, economically and in terms of content selection in comparison with older media (cf. Zillien and Haufs-Brusberg 2014, 74; van Dijk 2013, 34). What is available online is characterised by a great degree of heterogeneity and variety and is too vast to be structured by journalists as gatekeepers before reaching users (cf. Zillien and Haufs-Brusberg 2014: 74). A digital divide exists in relation to skills, technical equipment, frequency of use and content consumed. Moreover, access to and use of information technologies depends on socio-demographic factors such as income, education, job position, age, gender and ethnicity (cf. Van Dijk 2013, 29; Zillien and Haufs-Brusberg 2014, 81).

1.1 The Digital Economy and Society Index

Austria found itself ranked tenth among European Union countries in the *Digital Economy and Society Index* (DESI) ranking list in 2017. The index takes the following factors into consideration (cf. European Commission 2017a, 1):

- *Public digital services*: e-government/electronic government services.
- *Human capital*: Internet use, basic digital competence and advanced digital competence
- *Connectivity*: provision with fixed-line and mobile broadband, broadband speed and price
- *Integration of digital technology*: degree of digitalisation of the economy, electronic commerce
- *Internet use*: use of content, communication and online transactions by citizens

Taking into consideration the entirety of digital development, Austria is amongst the groups of countries with medium results. The other countries in this category are Germany, France, Latvia, Lithuania, Malta, Portugal, Slovenia, Spain and the Czech Republic. When considering factors in which Austria performed well overall, a digital split with respect to education, income and age becomes evident. The specific problem areas are discussed below.

In comparison with all other EU countries, Austria performs well primarily in the area of *public digital services*. Austria ranks fifth in this area (cf. European Commission (2017a, 9). Specifically, 38.3 per cent of Internet users have already filled out a form and sent it to a public institution online at least once (cf. ibid).

Clear differences manifest in relation to education level. While 42.4 per cent of all highly educated Austrians are aware of government services online, this is true of only 16.8 per cent of lower-educated Austrians (cf. European Commission 2017b, n.p.). Differences also become apparent with respect to household income: 37.9 per cent of persons from households with high incomes are already aware of e-government services. The level is only 29.4 per cent for those with low household incomes (cf. ibid). Even where Austria performs well in comparison with other EU countries in terms of making use of digital public services, there is a digital divide due to education and household income.

Austria is also above the EU average in the area of human capital; 82 per cent of Austrian residents use the Internet, which is somewhat higher than the EU average of 79 percent. Austrians also demonstrate at least basic digital skills more often[112] (65 per cent) than the EU average (56 per cent). However, there is a wide digital divide with respect to use and skills. While 98.5 per cent of 16 - 24-year-olds use the Internet regularly, only 58.5 per cent of 55 - 74-year-olds do. A digital divide also becomes apparent in connection with education. Regular Internet use is reported amongst 95.8 per cent of persons with a high level of education but just 58.2 per cent of those with a low level of education. There is also a discernible gap when it comes to household income, though this is not so obvious as with other factors: 88.8 per cent of individuals from high-income households and 77.9 per cent of individuals from low-income households use the Internet regularly (cf. European Commission 2017b, n.p.).

There are stark differences in digital competence between age groups. In the 16 - 24-year-old age group, 90.8 per cent possess basic digital skills. In the 25 - 54-year-old age group, the figure is only 72.9 per cent, and it is only 39 per cent in the 55 - 74-year-old age group. A stark digital divide is also apparent in the area of education. While 87.7 per cent of more highly educated persons have digital skills, this is the case for only 36.1 per cent of those with lower education. The same phenomenon can be observed with respect to household income. Of people living in high-income households, 73.9 per cent have basic digital skills, while only 53.1 per cent of those from low-income households possess such skills (cf. European Commission 2017b, n.p.).

Austria is also somewhat above the EU average in the *integration of digital technology*. While an average of 36 per cent of companies in EU countries exchange information electronically, this is the case for 41 per cent of Austrian companies. However, although 93 per cent of large companies[113] exchange information electronically, only 40 per cent of small and medium-sized companies do so[114] (cf. European Commission 2017b, n.p.).

Austria is close to the EU average for Internet use; 13 per cent of Austrians have not yet used the Internet (EU average: 14 per cent). While amongst the more highly

[112] Basic digital skills are, for example, the use of email services, editing tools, the ability to instal new devices, etc. (cf. European Commission 2017c, n.p.)
[113] At least 250 employees
[114] Ten to 249 employees

educated only 2.5 per cent have never yet used the Internet, the figure is 33 per cent for those with low education. 7 per cent of persons from high-income households and 16 per cent of persons from low-income households have not yet used the Internet. This is significantly fewer persons than the EU average (29 per cent). There is also a positive correlation between the age and quantity of 'offliners'. While just 0.5 per cent of 16 - 24-year-olds have never been online before, the figure is 7 per cent for 25 - 54-year-olds and 31 per cent for 55 - 74-year-olds (cf. European Commission 2017b, n.p.).

A total of 66 per cent of Austrian 'onliners' and 56 per cent of Austrians in general consume news on the Internet (EU average: 70 per cent, respectively 58 per cent). Of Austrians with a high level of education, 74 per cent read online newspapers, while this figure is only 34 per cent for those with a low level of education. In this area, the figure for use is also lower in older population groups: amongst 16 - 24-year-olds, 77 per cent read newspapers on the Internet; the figure is 62 per cent for 25 - 54-year-olds and 35 per cent for 55 - 74-year-olds (cf. European Commission 2017b, n.p.).

1.2 Digital divides

Even if Austria performs relatively well with regard to digitalisation in comparison with other EU countries and belongs to the group of 'digital followers' (along with Belgium, Germany, Ireland, Malta, Poland, Portugal, Slovakia, Spain and the UK; cf. Cruz-Jesus, Oliveira and Bacao 2012, 284), when the correlation between socio-demographic factors and actual use, respectively digital skills, is considered, a digital divide becomes apparent within Austria. This observation supports Jan van Dijk's thesis from 2005, which says that 'the digital divide is deepening where it has stopped widening' (van Dijk 2005, 2). According to this, a difference in use and skills is exhibited in regions where access to the Internet is widely distributed, (cf. van Dijk 2005, 2).

The exclusion of a part of the population from digitalisation is problematic because the public life of the community is increasingly being organised digitally. Citizens' individual lifestyle options therefore depend on the use of the Internet. Social status is also increasingly influenced by Internet use and digital skills: 'The ways in which we use the Internet, our skills and digital background, our digital and social capital, all influence our social status' (Ragnedda 2017, 73). Specifically, digital exclusion affects economic (e.g. job seeking), social (contacts), political (elections and other types of

political participation), cultural (participation in a cyber-culture) and spatial contexts (skills, leading a mobile life), and it affects institutional areas (realisation of civil rights) (cf. van Dijk 2013, 35).

Table 1: Austria's Digital Divide

	Education		**Income**		**Age**	
	High	Low	High	Low	Younger (18 - 24)	Older (55 - 74)
Submitting a form online	42.4	16.8	37.9	29.4	-	-
Regular Internet use	95.8	58.2	88.8	77.9	98.4	58.5
Basic digital skills	87.7	36.1	73.9	53.1	90.8	39.0
Has not yet used the Internet	2.5	33	7	16	0.5	31
Consumption of online news	74	34	-	-	77	35
Online banking	73	24	61	50	56	30

Source: European Commission

2. The results of the expert survey

The surveyed experts identified disadvantages at the personal, economic and democratic policy-making levels with which offliners consider themselves to be confronted, whereby economic disadvantages are considered to be the biggest limitations.

2.1 The individual

At the personal level, one representative from Safer Internet sees Austrians who are not digitally educated as challenged; she says that older persons often rely on support from children, acquaintances or others, e.g. when operating travel ticket machines. This gives them the feeling of having lost connection. Access to (practical) information is also made more difficult for offliners; for example, handbooks and operating instructions are often only available online now. Bills (e.g. telephone bills) are also being sent offline less and less, as one academic expert noted.

The representative from the C3W cites the tuition fees of students, for which information is only available online, as a specific example: 'Those who don't check their inboxes don't even know whether or when amounts are to be paid.' Another problem in this context for students, and for schoolchildren as well, is when they are required to use services and messengers the data protection measures of which are classified as doubtful, such as WhatsApp or Facebook groups. This means that even 'digital natives' who grew up with Internet use and as a rule are comfortable with it are put at a disadvantage if they don't want to consent to the use of questionable services.

Additional specific everyday limitations arise due to the decreasing number of rural bank branches and the fees that are charged more often for offline services, as respondents from the ORF, academia and epicenter.works note.

Those who cannot or will not access information online run the risk of an information deficit, warns one media expert. According to representatives of the Democracy Centre Vienna, ZARA and Safeinternet.at, the resulting drawbacks include higher expense for visits to authorities, an education deficit, harm to the labour market (lacking digital qualifications) and lacking digital networking that is important for professional development. Representatives of ISPA see a negative dynamic in this area on the labour market that scarcely grants chances of advancement to lower-educated persons.

2.2 The economy

At the economic level, offliners must cope with disadvantages in terms of price and time when purchasing products, according to the assessment of a respondent from the ORF. Price comparisons and the ability to view ratings online would clearly be simpler and accessible to the population at large, which is stressed by the representatives from nic.at and the C3W. Offline customers would be at a disadvantage here with respect to

information. One such disadvantage is created when long waiting times and inadequately trained personnel are encountered when consumers use the service and support hotlines of Austrian companies, notes the representative of the C3W. In her observation, offliners are also confronted with disadvantages in terms of price and time when booking flights and trips. Utilising the services of travel agents is often more expensive and time-consuming and requires the consumer's physical presence.

It is also becoming increasingly common that offers cannot be taken advantage of without the use of online tools. In this context, the representative from the C3W cites automobile-sharing service car2go, which requires an app that in turn accesses location data.

For companies, it is problematic that organisations are forced, regardless of their size, to use FinanzOnline since there is no longer any offline version available and invoices to public administration can only be submitted electronically via an online tool.

2.3 Democracy

With respect to democratic policy, the experts estimate that the digital divide is not yet a threat. Previously, the public authorities, for example, excluded no one with their 'You Can Use Online Services But You Don't Have To' approach, says the representative of the C3W. But the problems are already becoming apparent. Offliners generally have a more difficult time accessing information, are less connected and are put at a disadvantage with regard to mobilisation options. A representative of the Democracy Centre Vienna cites non-participation in online campaigns, such as those for the signing of petitions, as a concrete example.

From a democratic policy perspective, the availability and use of relevant information is vital. A respondent from the ORF assumes that the distribution of information via the media will be so strongly digitalised in future that offliners will have to contend with severe disadvantages. Representatives from nic.at specifically cite the expected decline in variety or even disappearance of print media; one academic expert adds encrypted digital antenna television and the changeover to digital radio.

Offliners will also have more difficulty making their opinions heard, notes a representative of the Democracy Centre. A representative of the ORF phrases it in concrete terms: *'If people's interests – the official "public opinion" – are observed primarily by analysing private data from online communication, offliners will become*

“voiceless” [and], consequently, underrepresented’. This can in turn lead to exclusion, fragmentation and stratification and threaten participation in democratic decisions, say experts from the New Institute for Culture Technologies and academia. In this context, an ORF representative emphasises that ‘it is imperative that public communication...[must] remain open to all segments of the population and at least make a claim of being understood, perceived and used by all’. In his opinion, segmentation due to deepening of the digital divide is to be expected, which will significantly weaken democracy.

2.4 Measures

The surveyed experts view the previous measures taken to combat the digital divide as insufficient. A representative from epicenter.works levels the criticism that sensitising initiatives by the federal government for digitalisation are often no more than advertising for individual companies. He cites the ‘digital roadmap’ as an example, for which a lobbying agency was commissioned to organise civic involvement in Austria. Representatives of the VAP, the C3W and ZARA see mainly civil society as active players on this field. While the initiatives were positive, a representative from the Institute for Culture Technology says that they were not enough.

A representative of the Digital Society sees a problem primarily in the fact that life-long learning is not enshrined in Austrian culture, which is necessary with regard to digitalisation. For one thing, the state is challenged to inspire a change in thinking, and for another, citizens must also be given opportunities to continue their education. This must include the entire education system, right up to adult education centres. Funding for safe and competent interaction with the Internet and the corresponding services for the necessary media competence are estimated to be insufficient by the experts. A spokesperson from the VÖZ finds that media competence education is available only to a very rudimentary extent at the moment and measures to increase competence have been neglected. The VÖZ, the C3W, ISPA and the Institute for Culture Technologies especially criticise the lacking training and continued education of teachers in the area of media competence and the lacking requirement for schools to impart media competence. In addition, the representative of the C3W notes that, along with specialised education, the technical equipment at schools is also inadequate, especially supplies of fibre optics.

Along with public institutions, at least partial responsibility for community media competence training is ascribed to the media.

The spokesperson from the VÖZ cites the ‘Zeitung in der Schule’ [Newspaper in Schools] project as a positive example. One academic expert also sees potential in traditional work to spread information on public service television, for example through TV instruction broadcasts.

3. Conclusion

Access to and exchange of information is significantly supported and facilitated by the Internet. This results in both benefits for society and drawbacks for individuals who are excluded from digitalisation.

In Austria, there are differences in usage, primarily between lower-educated and higher-educated persons, those with lower incomes and those with higher incomes, and between younger people and older people. Persons who do not participate in digital life also experience disadvantages in the offline world. From an economic perspective, offliners must cope with time and price disadvantages.

Austria is also confronted with problems in terms of democratic policy, which are caused by opinions not being heard, but also by lacking media competence. The fact that only a third of lower-educated Austrians have basic digital skills is alarming in an age of algorithms, filter bubbles and fake news. In order to counteract this problematic trend, both civil society initiatives must be promoted, and government measures must be taken. This includes promoting a culture of life-long learning and fostering media competence in kindergartens and schools up to technical colleges and universities, which can be achieved not only with improved training for teachers but also with sufficient technical equipment.

D. Summary evaluation in ten theses

In the understanding of Recommendation of the Council of Europe CM/Rec(2016)5, Internet freedom is largely guaranteed in Austria. Neither the analysis of the legal requirements and conditions nor the contemplation of civil society assessments have unearthed any serious restrictions. The results of this investigation are summarised in ten theses below.

1. Internet freedom as a fundamental right

Freedom of the Internet in Austria is assured in a broad and robust manner at the constitutional level through the fundamental rights of free speech, freedom of information and freedom of the media. These fundamental rights protect the use of the Internet, and indeed, with respect to the use of the associated technical infrastructure, access to the Internet and free communication using the Internet. The corresponding fundamental rights are guaranteed in provisions of Austrian
constitutional law and in Article 10 of the European Human Rights Convention. The fact that the European Human Rights Convention and its relevant guarantees are ranked at the constitutional level in Austria and grant subjective rights that are enforceable in court is especially significant. This fundamental rights protection is supplemented by the applicable fundamental rights in the Charter of the Fundamental Rights of the European Union.

2. Access to the Internet

There are no significant legal barriers to Internet access under Austrian law. Free access is guaranteed at the constitutional level by the aforementioned fundamental rights of free speech and freedom of the media. It is shaped by corresponding regulations of the Telecommunications Act and the Media Act, which ensure that access to, and use of, the Internet are open to any person without official permission within the framework of specific regulatory actions.

3. Blocking

Websites are not blocked or filtered in Austria due to official government decrees. However, the owners of copyright-protected rights, supported by corresponding authorisation under the Copyright Act, can (also) assert claims for injunctive relief vis-

à-vis ISPs, which must take appropriate measures to ensure that users do not unlawfully access protected content. Even if this mechanism complies with the requirements of constitutional and EU law on principle, especially with respect to the preservation of the rights of data subjects and the option to obtain relief, there are not insignificant legal uncertainties, especially on the side of the provider, and practical legal protection gaps in this context.

There are indeed security measures available under media law in order to remove illegal content on the Internet by deletion, provided that the content is distributed via online media that are governed by the Media Act. However, functional equivalents to the traditional mechanisms under media law for seizure and confiscation that account for the peculiarities of the Internet are lacking. As long as the private stakeholders alone, that is, primarily the providers, are the ones to enact blocking without sufficient judicial controls, there is a risk of 'over-blocking' and 'the imperative for constitutional proceedings is not sufficiently accounted for.

This likewise exhibits the limitations of 'self-regulation' by private stakeholders, which should only be relied upon if they are implemented using transparent procedures and with the rights of data subjects being protected. A current attempted reform to legal policy, through which providers should be authorised in the form of an extremely vague regulation to take measures to secure traffic as per article 3 of the TSM Regulation in order to prevent only generally cited 'criminally relevant behaviour' (on this, see p. 38 and footnote 67), is being registered with anxiety.

4. Net neutrality

The guarantee of unhindered and discrimination-free access to the Internet is ensured in Austria by the direct applicability of the EU regulation on measures pertaining to access to the open Internet. However, questions on details with respect to the scope of traffic management in general and traffic-securing measures in particular remain unanswered. With regard to such measures, there is neither transparency nor an obligation for operators to provide information, and it is at their discretion what level of service quality they guarantee based on technical requirements and how long they regard restrictions, if any, as necessary. Such activities of service providers, which should be limited to technical requirements, seem to be insufficiently scrutinised. However, whether effective scrutiny measures would be at all necessary and reasonable

cannot yet be assessed at the present time. Actual practice should be observed with heightened attention by stakeholders in politics, administration, the economy and civil society, in any case. Restrictions to Internet freedom resulting from this should not be ruled out.

5. Regulating content

The report gives an overview the applicable criminal and civil regulations that set the limitations of lawfulness for Internet communication for the purpose of content regulation. They include severe encroachments upon personality rights (abuse, invasion of privacy), penalise severe forms of incitement and make certain manifestations of cyber-stalking and cyber-bullying punishable. The courts take the guarantee of free speech into account in the enforcement of these offence definitions, so overreaching and disproportionate restrictions to this freedom are not a risk on principle. In the opinion of the surveyed stakeholders from civil society, the case law of the Austrian courts also does not give cause for complaint. The applicable criminal-law limitations are viewed as essentially sufficient. Problems of actual enforcement can arise, primarily in connection with abusive language and other encroachments on personality rights, especially with respect to the extraterritoriality and lack of borders of the Internet and the not insignificant costs of prosecution.

As yet, hate speech has not reached an extent in Austria that would make measures that exceed the protection ensured by the criminal legislature necessary. However, from a commercial perspective, programmed applications that open up echo chambers and filter bubbles in which differing opinions are systematically excluded are a threat to equitable public discourse. Even if such intrinsically closed communication spaces are not a new development, the easy accessibility and broad distribution offered by the Internet lends this phenomenon additional significance. The phenomenon of mass-distributed fake news, which is likewise not in any way new, has experienced an undesired intensification through the mechanism of echo chambers.

Online content that is illegal, or even abusive, injurious, offensive or demeaning, can be reported to various authorities in Austria. This reporting system, which is partly public and partly organised through civil society, generally functions effectively. The cooperation between these reporting offices and government officials (such as prosecutors) can and should be improved further. When illegal content is reported to police departments, trained and competent officials are occasionally lacking.

The restrictions of the public service broadcaster under the ORF-G represents a special case in the assessment of the restriction of Internet content. The removal of content seven days after it is broadcast, and any quantitative restriction of online postings and reports, represent a significant restriction of Internet freedom not only for the ORF but also for citizens.

6. The right to information

The fact that the right to official secrecy remains enshrined in Austrian constitutional law and that in practice there are still some exaggerated beliefs about the scope of government secrecy is rightly criticised in public debate. Reform has been sought for a long time and aims to pass a freedom of information law that would comprehensively oblige the authorities to provide information on all public matters and should grant citizens the right of access to information. However, more specific details on the drafting of this claim is the subject of ongoing discussion, and the fate of this draft is still open.

7. Data protection and privacy

The protection of privacy is under increasing pressure in Austria due to digital technologies. This is particularly clear in the use of smartphones because of their wide distribution (primarily amongst young people). Data protection problems due to cloud services, but above all due to big data applications, are less obvious, yet no less pressing.

The General Data Protection Regulation (GDPR) and the Austrian Data Protection Amendment Act cover many of these challenges, thereby contributing to better future protection of privacy in Austria. However, effective enforcement will be crucial. Practical testing of the new data protection legal framework is thus awaited. Even now there is scepticism regarding whether the GDPR will resolve fundamental questions about contemporary data protection.

The tension between data protection and the freedom of journalistic, academic, literary and artistic activities has not yet sufficiently been resolved by the Data Protection Amendment Act (section 9 DSG) because the statutory regulations outline the scope and applicability of exemption from provisions of the law only very vaguely.

Privacy protection in Austria is also marked by lacking awareness of problems, which is connected with the call to expand media competence. This affects not only

individuals but also companies and public institutions. Particularly public institutions are called upon to take on the role of forerunner for data protection in Austria.

8. Data protection, privacy and public security

As in all constitutional democracies, the tension between the requirements of public security in times of terrorism and serious criminal gang activity on the one hand and the proper protection of civil freedoms on the other poses special challenges in Austria. The police and judicial authorities are equipped with broad investigative measures through the corresponding laws that also enable access to traffic and location data of Internet communication, as well as – indeed only with judicial authorisation – surveillance of the content of Internet communication. However, the relevant surveillance measures are subject to scrutiny by the courts and special legal protection officers; the case law primarily of the Constitutional Court ensures that the constitutionality of the measures provided for under the law can be checked with respect to sufficient certainty of the laws and their necessity.

Current proposed reforms aim for a broader expansion of these powers. It is mainly the surveillance of Internet-based communication by the authorities that was provided for in a draft that has resulted in critical public discussions, regardless of the fact that this mechanism is meant to be utilised only with the existence of a justified suspicion that a crime has been committed and with an order from the public prosecutor and judicial approval.

9. Actual accessibility

The gap between access and actual use of the Internet known as the ‘digital divide’ has lost significance in Austria in the last two decades. The by far overwhelming proportion of households have access to an Internet connection of broadband quality (grid-bound or mobile). Those who live in households without an Internet connection can obtain access to the Internet in easily accessible public institutions. However, socio-economic differences remain. Significant differences in user competence are apparent along the lines of formal education, income and age; gender plays hardly any role. However, these stratified differences mean that the problems of the digital divide will not resolve themselves with the passage of time. The growing quantity of public and private services that are offered and can be made use of only over the Internet is putting people who lack Internet competence at an increasing disadvantage. When

digital mechanisms for participating in the democratic decision-making process (e.g. all forms of electronic voting) are designed, these people should be taken into account, including over the long term.

10. Digital media competence

The expansion of Internet competence is a prerequisite for being able to make full use of Internet freedom, and being able to arm oneself against the challenges that present themselves when this freedom is exercised. This expansion is the responsibility of individuals, on the one hand, and on the other the state has a duty to enable individuals to obtain competence. Educational institutions, from elementary schools to colleges, are central, but institutions of adult education and lifelong learning are also crucial. Digital competence means not only mastering application interfaces, but also building knowledge and understanding of function, institutional structures and the rights, duties and challenges associated with use. Only when building such competence is implemented comprehensively can positive Internet freedom and overcoming the digital divide in Austria be discussed.

Participating experts

(Listed alphabetically by surname)

Konrad Becker, World Information Institute / Institute for New Culture Technologies

DI Barbara Buchegger, ÖIAT - Austrian Institute for Applied Telecommunications / Saferinternet.at

Ing. Mag. Johann Čas, Institute for Technology Assessment

Mag. Dr Bernhard Collini-Nocker, Computer Sciences, University of Salzburg

Dipl. Kffr. Corinna Drumm, VÖP – Association of Association of Austrian Commercial Broadcasters

Monique A. Goeschl, VAP – Association for Anti-piracy in the Film and Video Industry

Mag. Gerald Grünberger, VÖZ - Association of Austrian Newspapers

Mag. Andreas Gruber, ISPA – Internet Service Providers Austria

Ing. Werner Illsinger, Digital Society Association

Margot Kapfer, Democracy Centre Vienna

Dr Ursula Maier-Rabler, Deputy Head of ICT&S – Center for Information and Communication Technologies & Society, Department of Communication Studies, University of Salzburg

Konrad Mitschka BS, ORF, Executive Department for Public Value staff

Mag. Dr Walter Peissl, Deputy Director of the Institute for Technology Assessment

Mag. Christian Pilnacek, Head of the Department of Criminal Law at the Federal Ministry of Justice (Section IV)

Mag.a Carmen Prior, Responsible Department Head at the Federal Ministry of Justice

Dr Gerhard Rettenegger, Head of 'Future Lab Online', ORF Salzburg, University Lecturer, Digital Salzburg Initiative

Claudia Schäfer MA, ZARA – Civil Courage and Anti-racism Work

Mag. Robert Schischka, Executive Director of nic.at, Head of the Austrian Computer Emergency Response Team

Dr Maximilian Schubert, Executive Director of ISPA – Internet Service Providers Austria

Florian Skrabal, Executive Editor of *Dossier*

Erwin Ernst Steinhammer, epicenter.works (formerly AKVorrat)

Mag. Dr Thomas Steinmaurer, Head of ICT&S – Center for Information and Communication Technologies & Society, Department of Communication Studies, University of Salzburg

Mag. Stefan Strauss, ITA – Institute of Technology Assessment

Richard Wein, Commercial Executive Director of nic.at

Dr Klaus Unterberger, ORF, Head of the Public Value Competence Centre

Dr Fritz Zeder, Head of a criminal legislation department at the Federal Ministry of Justice

Mag.a Daniela Zimmer, Data Protection Expert at the Chamber of Labour Vienna

Mag.a Klaudia Zotzmann-Koch, C3W – Chaos Computer Club Vienna

Literature

Access Info Europe & Centre for Law and Democracy (2016): Global Right to Information Rating. Online at: http://www.rti-rating.org/ (08/12/2017)

Afful-Dadzie, Eric and Afful-Dadzie, Anthony (2017): *Liberation of Public Data: Exploring Central Themes in Open Government Data and Freedom of Information Research.* In: International Journal of Information Management. Vol. 37(6). 66472

Akdeniz, Yaman (2016): *Media Freedom on the Internet: An OSCE Guidebook.* The Representative on Freedom of the Media. OSCE. Vienna. Online at: http://www.osce.org/fom/106285 (08/12/2017)

Akdeniz, Yaman (2012): *Freedom of Expression on the Internet.* Online at: http://www.osce.org/fom/80723?download=true (08/12/2017)

Berghel, Hal (2017): *Lies, Damn Lies, and Fake News.* In: Computer, 50th edition, book 2, 80-85.

Bezemek, Christoph (2017): *Hate Speech, Shitstorm und Dschihad Online: Müssen die Grenzen der Meinungsfreiheit neu vermessen werden?* In: Berka, Walter; Holoubek, Michael and Leitl-Staudinger, Barbara [ed.] *Meinungs- und Medienfreiheit in der digitalen Ära: Eine Neuvermessung der Kommunikationsfreiheit.* Schriftenreihe Recht der elektronischen Massenmedien. Volume 15. Manz´sche Verlags- und Universitätsbuchhandlung. Vienna.

Brodnig, Ingrid (2017): *Lügen im Netz. Wie Fake News, Populisten und unkontrollierte Technik uns manipulieren.* Christian Brandstätter. Vienna.

Brown, Tracy (2013): *Blogger or Journalist? Evaluating what is the press in the digital age.* New York: The Rosen Publishing Group.

Bundeskanzleramt (2017): Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Mediengesetz, version as at 06/09/2017. Online at: https://www.ris.bka.gv.at (08/12/2017).

Burgstaller, Manfred and Kurbarth, Louis (2016): *Core data of the legal protection officer for 2015.* In: Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (SIAK Journal). March 2016 edition.

Cannataci, Joseph A.; Zhao, Bo; Torres Vives, Gemma; Monteleone, Shara; Mifsud Bonnici, Jeanne and Moyakine, Evgeni (2016): *Privacy, free expression and*

transparency. Redefining their new boundaries in the digital age. UNESCO Series on Internet Freedom, Paris. Online at: http://unesdoc.unesco.org/images/ 0024/002466/246610e.pdf (08/12/2017)

Čas, Johann; Bellanova, Rocco; Burgess, J. Peter; Friedewald, Michael and Peissl, Walter (2017): *Introduction. Surveillance, privacy and security.* In: Friedewald, Michael; Burgess, J. Peter; Čas, Johann; Bellanova, Rocco and Peissl, Walter (eds.) *Surveillance, Privacy and Security. Citizens Perspectives.* Routledge. London / New York.

Castells, Manuel (2000): *The Rise of the Network Society.* Second edition. Oxford: Blackwell.

CERT (Computer Emergency Response Team; 2017): Österreichische Strategie für Cyber Sicherheit. *Update.* Online at: https://www.cert.at/reports/ report_2015_ chap07/content.html (08/12/2017)

Computer Emergency Response Team Austria (2016): Bericht Internet-Sicherheit Österreich. [Report on Internet Security in Austria] Complete edition. Online at: https://cert.at/static/downloads/reports/cert.at-jahresbericht-2016.pdf (08/12/2017)

Christl, Wolfie (2014): *Kommerzielle digitale Überwachung im Alltag. Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele.* Cracked Labs. Institut für kritische digitale Kultur. Vienna; on behalf of the Federal Chamber of Labour. Online at: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (08/12/2017)

Coe, Peter (2015): *The Social Media Paradox: An Intersection with Freedom of Expression and the Criminal Law.* In: Information & Communications Technology Law.

Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 28 January 2003, art. 5 para. 1.

Council of Europe, Committee of Ministers (1997): Recommendation No. R (97) 20 of the Committee of Ministers to Member States on “Hate Speech”. Online at: https://rm.coe.int/1680505d5b (08/12/2017)

Council of the European Union (2008): Council Framework Decision 2008/ 913/ JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Cruz-Jesus, Frederico; Oliveira, Tiago and Bacao, Fernando (2012): *Digital divide across the European Union.* In: *Information & Management*, 49th edition, n.p., 278-291.

Dutton, William; Dopatka, Anna; Hills, Michael; Law, Ginette and Nash, Viktoria (2015): *Freedom of Connection. Freedom of Expression. The Changing Legal and Regulatory Ecology Shaping the Internet.* UNESCO Series on Internet Freedom. Paris. Online at: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publicationsby-series/unesco-series-on-internet-freedom (08/12/2017)

Eldrige II, Scott A. (2017): *The Digital Journalist. The journalistic field, boundaries, and disquieting change.* In: Franklin, Bob and Eldridge II, Scott A. (ed.): The Routledge Companion to Digital Journalism Studies. Routledge. London/New York, 44-63.

European Commission (2017a): Europe's Digital Progress Report 2017 - Country Profile: Austria. Online at: https://ec.europa.eu/digital-singlemarket/en/scoreboard/austria (08/12/2017).

European Commission (2017b): See the evolution of an indicator and compare countries. Online at: http://digital-agenda-data.eu/charts/see-the-evolution-of-anindicator-and-compare-countries#chart (08/12/2017).

European Commission (2017c): The Digital Economy and Society Index (DESI). List of Indicators. Online at https://ec.europa.eu/digital-single-market/en/desi (08/12/2017).

European Court of Human Rights (2012): Case of Ahmet Yildirim v. Turkey 3111/ 10 dated 18/12/2012

European Union (2016): Flash Eurobarometer 443 e-Privacy: Austria. Online at: https://data.europa.eu/euodp/data/dataset/S2124_443_ENG (08/12/2017]

European Parliament and Council of the European Union (2015): Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

European Parliament and Council of the European Union (2013): Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

European Parliament and Council of the European Union (2000): Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internat Market ("Directive on electronic commerce").

Ferrara, Emilio (2015) "Manipulation and abuse on social media" by Emilio Ferrara with Ching-man Au Yeung as coordinator. ACM SIGWEB Newsletter, (Spring), 1-9

Froitzheim, Ulf J. (2017): *Echokammern sind nicht harmlos.* In: Kappes, Christoph and Krone, Jan/Novy, Leonard (ed.): *Medienwandel kompakt.* 2014-2016. Wiesbaden: Springer Fachmedien, 105-108.

Fürst, Silke; Schönhagen, Philomen and Bosshart, Stefan (2015): *Mass Communications is more than a one-way street: on the persistent function and relevance of journalism.* In: Javnost: *The Public*, 22nd edition, book 4, 328-344.

Gagliardone, Ignio; Gal, Danit; Alves, Thiago and Martinez, Gabriela (2015): *Countering Online Hate Speech.* UNESCO Series on Internet Freedom. Paris. Online at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf (08/12/2017).

Gadringer, Stefan; Sparviero, Sergio; Trappel, Josef; Büchner, Jana and Holzinger, Roland (2017): Reuters Digital News Report – Detailergebnisse für Österreich 2017. Online at: https://www.uni-salzburg.at/index.php?id=205115 (08/12/2017).

Gadringer, Stefan; Sparviero, Sergio; Trappel, Josef and Wenzel, Corinna (2016): Reuters Digital News Report – Detailergebnisse für Österreich 2016. Online at: https://www.uni-salzburg.at/index.php?id=205115 (08/12/2017).

Gersdorf, Hubertus (2009): *Auswirkungen der Medienkonvergenz auf den Rundfunkbegriff und die Medienregulierung.* In: Gundel, Jörg; Heermann, Peter W. and Leible, Stefan (ed.): *Konvergenz der Medien – Konvergenz des Rechts?* JWV Jenaer Wissenschaftliche Verlagsgesellschaft mbH. Sipplingen, 31-45.

Gründhammer, Veronika (2014): *Facebook, Twitter und Co.: Netze in der Datenflut?* In: Ortner, Heike; Pfurtscheller, Daniel; Rizzolli, Michaela and Wiesinger, Andreas
(ed.): *Datenflut und Informationskanäle.* Innsbruck University Press. Innsbruck, 71-82.

Harsin, Jayson (2015) *Regimes of Posttruth, Postpolitics and Attention Economies.* In: *Communication, Culture & Critique, 8/ 2015, 327-333.*

Heinisch, Reinhard C. (2009): *Der demokratische Marktplatz der Meinungen: Ideal und Realität im digitalen Zeitalter*. In: Berka, Walter; Holoubek, Michael; Leitl-Staudinger, Barbara [ed.] *Meinungsvielfalt im Rundfunk und in den OnlineMedien.* Schriftenreihe Recht der elektronischen Massenmedien. Volume 12. Manz´sche Verlags- und Universitätsbuchhandlung. Vienna.

Korff, Douwe and Brown, Ian (2013): *The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications.* Council of Europe. Online at:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2356797 (08/12/2017) Krieger-Lamina, Jaro (2016) *Vernetzte Automobile. Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. Endbericht*. Report no. 201602; Institute of Technology Assessment (ITA): Vienna; on behalf of: The Federal Chamber of Labour Online at: http://epub.oeaw.ac.at/ita/ita-projektberichte/2016-02.pdf (08/12/2017)

Lee, Yin Harn (2015): *Copyright and Freedom of Expression: A Literature Review.* CREATe Working Paper Series. College of Social Sciences/School of Law. University of Glasgow. Glasgow. Online at: http://www.create.ac.uk/publications/copyright-and-freedom-of-expression-a-literature-review/ (08/12/2017)

Lehofer, Hans Peter (2009): *Pluralismus unter den Bedingungen des Internet.* In: Berka, Walter; Holoubek, Michael; Leitl-Staudinger, Barbara [ed.] *Meinungsvielfalt im Rundfunk und in den Online-Medien.* Schriftenreihe Recht der elektronischen Massenmedien. Volume 12. Manz´sche Verlags- und Universitätsbuchhandlung. Vienna.

Mayerhofer, Michael (2017): *Google, Facebook & Co: Die Macht der Algorithmen aus grundrechtlicher Perspektive.* In: Berka, Walter; Holoubek, Michael; Leitl-Staudinger, Barbara [ed.] *Meinungs- und Medienfreiheit in der digitalen Ära: Ein Neuvermessung der Kommunikationsfreiheit.* Schriftenreihe Recht der elektronischen Massenmedien. Volume 15. Manz´sche Verlags- und Universitätsbuchhandlung. Vienna.

MacKinnon, Rebecca; Hickok, Elonnai; Bar, Allon and Lim, Hae-in (2015): *Fostering Freedom of Expression Online: The Role of Internet Intermediaries.* UNESCO Series on Internet Freedom. Paris. Online at: http://unesdoc.unesco.org/ images/0023/002311/231162e.pdf (08/12/2017).

Meikle, Graham and Young, Sherman (2012): *Media Convergence. Networked Digital Media in Everyday Life.* Hampshire, New York: Palgrave Macmillan.

Mendel, Toby; Puddephatt, Andrew; Wagner, Ben; Dixie, Hawtin and Torres, Natalia (2012): *Global Survey on Internet Privacy and Freedom of Expression.* UNESCO Series on Internet Freedom. Paris. Online at: http://unesdoc.unesco.org/images/0021/002182/218273e.pdf (08/12/2017)

Mihailidis, Paul and Viotty, Samantha (2017): *Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in 'Post-Fact' Society.* In: American Behavioral Scientist, 61st edition, book 4, 441-454.

Pariser, Eli (2012): *Filter Bubble. Wie wir im Internet entmündigt werden.* Carl Hanser Verlag. Munich.

Pfeifer, Karl-Nikolaus (2009): *Presserecht im Internet – Drei Thesen und eine Frage zur Einordnung, Privilegierung und Haftung der „elektronischen Presse"*. In: Gundel, Jörg; Heermann, Peter W. and Leible, Stefan (ed.): *Konvergenz der Medien –*

Konvergenz des Rechts? JWV Jenaer Wissenschaftliche Verlagsgesellschaft mbH. Sipplingen, 47-59.

Pick, James B. and Sarkar, Avijit (2015): *The Global Digital Divides. Explaining Change*. Springer. Berlin/Heidelberg.

Ragnedda, Massimo (2017): *The Third Digital Divide. A Weberian Approach to Digital Inequalities.* Routledge. London

Rothmann, Robert; Sterbik-Lamina, Jaro and Peissl, Walter (2014): *Credit Scoring in Österreich.* Report No. ITA-PB A66; Institute of Technology Assessment (ITA). Vienna; on behalf of: The Federal Chamber of Labour Online at: http://epub.oeaw.ac.at/ita/ita-projektberichte/a66.pdf (08/12/2017)

Rothmann, Robert; Sterbik-Lamina, Jaro; Peissl, Walter and Čas, Johann (2012): *Aktuelle Fragen der Geodaten-Nutzung auf mobilen Geräten – Endbericht.* Report No. ITA-PB A63; Institute of Technology Assessment (ITA). Vienna; on behalf of: Austrian Federal Chamber of Labour Online at: http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a63.pdf (08/12/2017)

Rundfunk und Telekom Regulierungs-GmbH (2017): *Netzneutralitätsbericht 2017 der RTR.* Online at: https://www.rtr.at/de/inf/NNBericht2017/Netzneutralitaetsbericht_2017_RTR.pdf (08/12/2017)

Shugurova, Irina and Shugurov, Mark V. (2016): *Copyright or Right-To-Copy? Towards the Proper Balance between Freedom of Expression and Copyright in Cyberspace.* In: Journal of Advocacy. Vol. 7(3). 148-157.

Schweiger, Wolfgang (2017): *Der (des)informierte Bürger im Netz. Wie soziale Medien die Meinungsbildung verändern.* Springer. Wiesbaden.

Svenson, Måns; Rosengren, Calle and Åström, Fredrik (2016): *Digitalization and Privacy: A systematic literature review*. Online at: https://lup.lub.lu.se/search/publication/017b3c44-be8e-40eb-a193-cc5bdd24cbc1 (08/12/2017)

Thies, Ben (2017): *Mythos Filterblase.* In: Kappes, Christoph and Krone, Jan/Novy, Leonard (ed.): *Medienwandel kompakt.* 2014-2016. Springer Fachmedien. Wiesbaden, 101-104.

Tschohl, Christof (n.y.): *Studie zum Konzept einer zentralen „Clearingstelle" zur inhaltlichen Beurteilung von Netzsperren im Zusammenhang mit Verletzungen des Urheberrechts.* Research Institute AG & Co KG. Zentrum für Digitale

Menschenrechte. Vienna; on behalf of Internet Service Providers Austria (ISPA). Online at: https://www.ispa.at/wissenspool/studien/studien-detailansicht/studienansicht/detail/netzsperren.html (08/12/2017)

UNESCO (2015): *Keystones to foster inclusive Knowledge Societies. Access to information and knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet.* Paris. Online at: http://www.unesco.org/new/en/ communication-and-information/resources/ publications-and-communicationmaterials/publications/publications-by-series/unesco-series-on-internet-freedom/ (08/12/2017)

Unterberger, Andreas (2017): *Zwischen Lügenpresse und Fake News. Eine Analyse.* Verlag Frank&Frei. Vienna.

van Dijk, Jan (2012): *The Network Society.* 3rd edition. London, Thousand Oaks, New Delhi, Singapore: Sage.

Van Dijk, Jan A.G.M. (2013): *A theory of the digital divide.* In: Ragnedda, Massimo and Muschert, Glenn W. (ed.): *The Digital Divide. The internet and social inequality in international perspective.* Routledge. London/New York.

Voorhoof, Dirk and Hannes, Cannie (2010): *Freedom of Expression and Information in a Democratic Society.* In: International Communication Gazette. Vol. 72, 4-5.

VÖP (2017): *Media Future Perspectives. Das Weißbuch für den Medienmarkt Österreichs.* Vienna. Verband Österreichischer Privatsender.

VÖZ (2017): *Rechtsinformationen.* Online at http://voez.at/politik-recht/rechtsinformationen (08/12/2017).

Wessels, Brigitte (2013): *The reproduction and reconfiguration of inequality. Differentiation and class, status and power in the dynamics of digital divides.* In: Ragnedda, Massimo and Muschert, Glenn W. (eds.): *The Digital Divide. The internet and social inequality in international perspective.* Routledge. London/New York.

Yannoukakou, Aikaterini and Araka, Iliana (2014): *Access to Government Information: Right to Information and Open Government Data Synergy.* In: Procedia – Social and Behaviorial Sciences, Vol. 147, 332-340.

Zillien, Nicole and Haufs-Brusberg, Maren (2014): *Wissenskluft und Digital Divide.* Nomos. Baden-Baden.

List of Abbreviations

ABGB	Allgemeines bürgerliches Gesetzbuch [Austrian General Civil Code] JGS [Austrian collection of judicial legislation] 1811/946, as amended
AMD-G	Audiovisuelle Mediendienste-Gesetz [Audiovisual Media Services Act] BGBl I 2001/84, as amended
AVMS Directive	Directive on audio-visual media services (2010/13/EU)
BGBl	Bundesgesetzblatt [Federal Law Gazette] (can be found at https://www.ris.bka.gv.at/Bund/)
BKA	Bundeskanzleramt [Office of the Federal Chancellor]
BMJ	Bundesministerium für Justiz [Austrian Federal Ministry of Justice]
B-VG	Bundesverfassungsgesetz [Austrian Federal Constitutional Act] BGBl 1930/1, as amended
C3W	Chaos Computer Club Vienna
CoE	Council of Europe
DESI	Digital Economy and Society Index
DPI	Deep Packet Inspection
DSG	Datenschutzgesetz [Data Protection Act] BGBl I 1999/165 as amended to BGBl I 2017/120.[115]
ECG	E-Commerce-Gesetz [Electronic Commerce Act] BGBl I 2001/152
ECtHR	European Court of Human Rights
ECHR	(European) Human Rights Convention BGBl 1958/210, as amended
EU-GDPR	European General Data Protection Regulation (Regulation (EU) 2016/679)
ECJ	European Court of Justice
CFR-EU	Charter of Fundamental Rights of the European Union OJ [Official Journal of the European Union] 2012 C 326, 391, as amended
ISP	Internet Service Provider
ISPA	Internet Service Providers Austria
ITA	Institut für Technikfolgenabschätzung [Institute of Technology Assessment]
KommAustriaG	KommAustria-Gesetz [Austrian Communications Authority Act]

[115] The DSG as amended to the Data Protection Amendment Act, BGBlI 2017/120, comes into effect together with the General Data Protection Regulation on 25/05/2018.

	BGBl I 2001/32, as amended
MedienG	Mediengesetz [Media Act] BGBl 1981/314, as amended
MR	Medien und Recht [Media and Law] Journal
OGH	Oberster Gerichtshof [Austrian Supreme Court of Justice]
ÖIAT	Österreichisches Institut für angewandte Telekommunikation [Austrian Institute for Applied Telecommunications]
ORF	Österreichischer Rundfunk [Austrian Broadcasting Corporation]
ORF-G	ORF-Gesetz [ORF Act] BGBl 1984/379, as amended
PStSG	Polizeiliches Staatsschutzgesetz [Police State-protection Act] BGBl I 2016/5, as amended
DR	Directive
SNS	Social Network Sites, also known as *social media*
SPG	Sicherheitspolizeigesetz [Federal Security Police Act] BGBl 1991/566, as amended
StGB	Strafgesetzbuch [Criminal Code] BGBl 1974/60, as amended
StGG	Staatsgrundgesetz über die allgemeine Rechte der Staatsbürger [Basic law on the general rights of citizens] RGBl [Imperial Law Gazette] 1867/142, as amended
StPO	Strafprozessordnung [Code of Criminal Procedure] 1975 BGBl 1975/631, as amended
TKG 2003	Telekommunikationsgesetz [Telecommunications Act] 2003 BGBl I 2003/70, as amended
TSM Regulation	Telecoms Single Market Regulation (Regulation (EU) 2015/2120)
UrhG	Urheberrechtsgesetz [Copyright Act] BGBl 1936/111, as amended
VerG	Vereinsgesetz [Associations Act] 2002 BGBl I 66, as amended
VersG	Versammlungsgesetz [Public Meetings Act] 1953 BGBl 98, as amended
VfGH	Verfassungsgerichtshof [Constitutional Court]
VfSlg	Ausgewählte Entscheidungen des Verfassungsgerichtshofes [Selected Decisions of the Constitutional Court]
VAP	Verein für Anti-Piraterie der Film- und Videobranche [Association for Anti-piracy in the Film and Video Industry]
VÖP	Verband Österreichischer Privatsender [Association of Austrian Commercial Broadcasters]
VÖZ	Verband Österreichischer Zeitungen [Association of Austrian Newspapers]
ZARA	Zivilcourage und Anti-Rassismus-Arbeit [Civil Courage and Anti-racism Work]

Appendix: Recommendation CM/Rec(2016)5

Recommendation CM/Rec(2016)5 of the Committee of Ministers to the member states on Internet freedom

(Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies)

1. The European Convention on Human Rights (ETS No. 5, hereinafter "the Convention") applies both offline and online. The Council of Europe member States have negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet.

2. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the Convention and the International Covenant on Civil and Political Rights. The member States of the Council of Europe should take a proactive approach to implementing the Convention and other Council of Europe standards with regard to the Internet. The understanding of Internet freedom should be a comprehensive one and firmly based on these standards.

3. Internet governance arrangements, whether national, regional or global, must build on this understanding of Internet freedom. States have rights and responsibilities with regard to international Internet-related policy. In the exercise of their sovereign rights, States should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities inside or outside of their jurisdiction. Any national decision or action restricting human rights and fundamental rights on the Internet must comply with international obligations and in particular be based on law. It must be necessary in a democratic society, fully respect the principles of proportionality and guarantee access to remedies and the right to be heard and to appeal with due process safeguards.

4. As part of their obligation to secure to everyone within their jurisdiction the rights and freedoms enshrined in the Convention, States should create an enabling

environment for Internet freedom. To this end, it is recommended that States carry out regular evaluations of the Internet freedom environment at the national level, with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop. Such evaluations contribute to a better understanding of the application of the Convention to the Internet in member States and to its better implementation by national authorities.

5. The Convention and other Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. They can be considered as indicators which guide and enable member States to identify existing or potential challenges to Internet freedom, as an analytical framework to evaluate the implementation of human rights standards on the Internet and as a reference for developing international policy and approaches relating to the Internet.

6. The Council of Europe should play a key role in promoting Internet freedom in Europe and globally. Building on member States' national evaluations, the Council of Europe can observe the evolution of regulatory frameworks and other developments in its member States and provide regular overviews on the challenges to Internet freedom in Europe. This would be a good basis for further development of Council of Europe Internet-related policies.

7. The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe, recommends that member States:

- periodically evaluate the level of respect for and implementation of human rights and fundamental freedom standards with regard to the Internet, using the indicators in the appendix to this recommendation, with a view to elaborating national reports, wherever appropriate;
- ensure the participation of all stakeholders from the private sector, civil society, academia and the technical community, in their respective roles, in the evaluation of the state of Internet freedom and preparation of national reports;
- consider sharing, on a voluntary basis, information or national reports on Internet freedom with the Council of Europe;

- be guided by and promote these indicators when participating in international dialogue and international policy making on Internet freedom;
- take appropriate measures to promote the United Nations “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect, and Remedy’ Framework”.